

Copy No: _____



Global Security Scan for Canadian Science Capabilities (2015 – 2020)

Report of Proceedings

March 21-23, 2007
Shirley's Bay, Ottawa

Lynelle Spring
SpringWorks Consulting

Robert Crawhall
National Capital Institute of Telecommunications

Jack Smith
Office of the National Science Advisor

Ken Andrews
High Impact Facilitation

Defence R&D Canada, Centre for Security Science

DRDC CSS CR 2008-06

March 2008

Lynelle Spring; Robert Crawhall; Jack Smith

Approved by

Alain Goudreau
DRDC CSS Risk Portfolio Manager

Approved for release by

Andrew Vallerand
Chair CSS Document Review Panel

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defense R&D Canada

Abstract

The purpose of this workshop was to provide a prospective on future challenges to Canadian public safety and national security in the time-frame of 2015 and beyond, identify capabilities for meeting these challenges, and examine opportunities presented by science and technology for generating the capabilities.

The “foresight” workshop engaged over fifty Canadian and foreign experts from industry and academia as well as from the British and Canadian governments.

Using an “all-hazards” approach to public safety and security, four areas of critical infrastructure were discussed: communications, finance, transportation, and energy distribution. Using “foresight” techniques, the workshop approached the complex inter-dependencies of these four critical infrastructures through three “lenses of vulnerability” – people, physical, and cyber.

Recommendations were made for the development of scientifically based capabilities for the security and protection of critical infrastructure. The core recommendations were seen as being relevant to all four areas of critical infrastructure and expected to be applicable to all other areas of infrastructure as well.

Résumé

Le but de cet atelier était de jeter un éclairage sur les défis de la sécurité du public et de la sécurité nationale en 2015 et au-delà, de déterminer les capacités requis pour relever ces défis, et d'examiner comment la science et la technologie peuvent fournir ces capacités.

L'atelier sur la « prévision » a réuni plus de 50 spécialistes canadiens et étrangers représentant l'industrie, le milieu universitaire, et les gouvernements du Canada et du Royaume-Uni.

Adoptant une approche « tous risques » en matière de sécurité du public, les participants ont examiné quatre secteurs de la protection des infrastructures essentielles : les communications, les finances, le transport et la distribution de l'énergie. À l'aide de techniques de « prévision » ils ont analysé les interdépendances complexes entre ces quatre secteurs selon trois « aspects de la vulnérabilité » : humain, matériel, et cyber.

Des recommandations ont été faites sur le développement de capacités fondées sur la recherche scientifique pour la sécurité et la protection des infrastructures essentielles. Les principales recommandations ont été jugées applicables aux quatre secteurs examinés, ainsi qu'à tous les autres secteurs de la protection des infrastructures essentielles.

This page intentionally left blank.

Executive Summary

On March 21, 2007, the Centre for Security Science at Defence Research and Development Canada – in conjunction with Public Safety Canada, the Office of the National Science Advisor and the National Capital Institute of Telecommunications – launched a three-day workshop. The event utilized Foresight and Scanning methodology to help participants develop advice on Canada's science needs with respect to "All-Hazards" threats in the 2015 to 2020 timeframe. Four areas of critical infrastructure protection (CIP) – Communications, Finance, Transport and Energy Distribution were explored in depth.

Fifty-four invited professionals were tasked with contributing to the workshop through a facilitated process that emphasized cross-disciplinary and cross-sectoral knowledge-sharing and consensus while taking advantage of individual expertise. Participants came from government, industry and academia, and care was taken to achieve a representative balance of expertise across the infrastructure areas and the threat environments.

Based on the experience of the 2006 Prospective Security Futures Scan this workshop approached the complex inter-dependencies of critical infrastructure protection through three "lenses of vulnerability" – People, Physical and Cyber.

Key observations were as follows:

- 1) The threat environment in 2015 will be significantly worse than today in terms of the severity of individual threats and particularly in terms of the summation of all threats to each infrastructure area.
- 2) To counter this enhanced threat environment, fundamental and systemic investments will have to be made in knowledge, technology and process.
- 3) Internationally, governments and the private sector are taking on distinct leadership roles in partnering for the future protection of critical infrastructure through research and innovation.
- 4) Science, including technology and the social sciences will play a critical role in meeting the 2015-2020 challenge.

The Enhanced Threat Environment

The workgroup represented a broad cross-section of knowledge with respect to the threat environment. A consistent message across the range of possible threats was that the risk to our critical infrastructure will be dramatically higher in the 2015 to 2020 timeframe. Using the three vulnerability lenses a capsule summary is as follows:

Human Infrastructure

People as victims

- The outbreak of disease such as avian flu or a flu pandemic is anticipated. The reliability and resilience of the critical infrastructure to prolonged, high-percentage absenteeism is un-quantified.

People as threat

- There will be significantly more groups and individuals with a wide range of motivations – notoriety, alienation, terror, crime, economic sabotage, political affiliation, etc. – with varying levels of access to physical and cyber technologies from state-sponsored to on-line freeware, networked into communities of malfeasance and continuously alerted to vulnerabilities in the critical infrastructure.

People as responders

- Deficiencies in inter-organizational cooperation will be a major exacerbating factor in the failure of prevention, response and remediation activities.

Physical Infrastructure

Climate change and ozone depletion are expected to result in aggravated weather conditions and greater solar interference.¹ In addition existing infrastructure is aging. There is possibly \$50 billion in deferred maintenance on existing infrastructure². New investment is not expected to represent a significant percentage of critical infrastructure by 2015.

Cyber Infrastructure

Communications

- The Internet and associated systems will increase in pervasiveness over the next decade. The underlying protocols and mechanisms (many of which are approaching thirty years old) are insufficient for the task of providing robust public infrastructure. To date comprehensive fixes for known Internet vulnerabilities have proven to be elusive and are not anticipated to take place prior to 2015. Overlay systems such as wireless access networks contribute further risks. Software is becoming increasingly complex and patchwork. Accountability for the system integrity is hard to establish. Outsourcing of software and communications systems for national communications infrastructure to foreign nations who may be in significant competition with Canada or Canadian-based industries in the 2015-2020 timeframe.

¹ Solar Cycle 24 will be 50% stronger than Cycle 23 lasting from approximately 2010 to 2018.

² Pro: <http://www.fcm.ca/English/documents/finSub.pdf> Con: http://www.cwf.ca/V2/cnt/bogusdeficit_9112.php

Other Critical Infrastructure

- In addition to increased dependency on the public communications infrastructure, internal networks and information technologies controlling critical infrastructure including supervisory control and data acquisition (SCADA) systems used in transportation and energy distribution will present new vulnerabilities. Global competitiveness, urban congestion, energy efficiency and other major trends are driving investment in operational information and communications technologies (ICT) much of which is similar to the technology underlying the communications infrastructure. SCADA systems are becoming hybrids of older systems and newer, Internet Protocol-based technologies. These hybrid systems have un-quantified security vulnerabilities. They are expected to be subjected to increasing levels of malicious cyber threat as well as lower reliability due to system complexity.

The threats and vulnerabilities described briefly above are considered irresistible and unavoidable. Simple technological fixes will not be sufficient. Investment is required in new knowledge to establish the capacity to mitigate the effects of these and other threats. Leadership in a number of these areas must come from the Public Safety community as market mechanisms are not expected to react to these potential events in a timely manner. Recommendations of the workgroup address these issues in a comprehensive and systemic fashion.

Key Recommendations Arising from the Workshop

1. Self-healing cyber systems

Cyber systems for critical infrastructure will have to be specified and designed to be robust against persistent and varied threats of both the intentional and unintentional varieties. Security must be as important as efficiency. Failure states must be benign. Software must be self auditing to ensure that processes are running properly and that no unanticipated activities are taking place. Intrusion detection must be seamless. Quantifiable "trust mechanisms" will be required for cyber transactions. Public and critical infrastructure enterprise communications and IT systems including SCADA systems must have seamless security strategies. The capacity and knowledge should be developed to effectively specify such systems and use government procurement power to drive industry specifications along with international allies.

2. Inter- and Cross-Cultural Collaboration

Building on experience in the UK and elsewhere, deep understanding of motivation, alienation and identity of groups within and outside Canadian society is essential to the prevention and detection of many potential hostile actions. Research should be undertaken leading to effective social policies related to CIP.

3. Inter-Organizational/ Augmented Collaboration, Exercises, Cognition and Ergonomics

Tools and techniques will be required to overcome historically entrenched silos of behaviour. In addition systems must be designed for error-free operation and trust-enhancing in times of crisis.

Physical exercises and practice sessions should take place as an essential element of developing effective tools, techniques and trust.

4. Complexity Science for Critical Infrastructure

Threats to critical infrastructure systems in the 2015-2020 timeframe will be exacerbated by their increasing and largely indeterminate complexity. Complexity science offers the potential of significant simplification in CIP approaches.

5. Infrastructure Planning and Redundancy Theory

Current redundancy strategies for protection of critical infrastructure presume random and independent events of limited scope. New practices are required which allow for intelligent interference and multiple events. Current threat-levels should be revised to reflect predicted climatic extremes and other changes rather than purely historical data and to allow for "intelligent" threats.

6. Sensors, Data Fusion & Data Mining

Information gathering and analysis using novel sensors (including new materials), data management techniques and visualization will be important tools in CIP. The knowledge and capacity to specify and manage these systems should be comparable to current voice and data systems.

Spring, L; Crawhall, R. 2007.

Global Security Scan for Canadian Science Capabilities (2015 – 2020): Report of Proceedings.

DRDC CSS CR 2008-06 Centre for Security Science.

Table of Contents

Abstract.....	i
Résumé	i
Executive Summary	iii
The Enhanced Threat Environment	iii
▪ Human Infrastructure	iv
▪ Physical Infrastructure	iv
▪ Cyber Infrastructure	iv
Key Recommendations Arising from the Workshop.....	v
1. Foreword.....	1
1.1 A Message from the Project Management and Advisory Team	1
1.2 Why S&T Foresight?	2
2. Context for the 2007 <i>Global Security Scan for Canadian Science</i> Workshop	5
2.1 Policy Environment, Conceptual & Methodological Frameworks	5
▪ Policy Environment	6
▪ Conceptual Framework	7
▪ Methodological Framework: Foresight & Security.....	8
2.2 Workshop Methodology	9
▪ Participation Framework	10
▪ Participant Skills & Expertise	11
▪ Lenses of Vulnerability	12
▪ Selection of Critical Infrastructure (CI) Sectors	14
▪ Cyber and Communications	14
▪ Role of the Social Sciences	15
3. Stimulus Presentations	16
3.1 Day 1 – Setting the Stage	17

	▪ Stephen Featherston	<i>Future Communications Security Considerations: A Telecom, Enterprise and Mobile Infrastructure Perspective</i>	17
	▪ Joseph Decree	<i>White Wolf Security Presentation</i>	20
3.2	Day 2 – Integration		22
	▪ Walter Derzko	<i>Smart Technologies</i>	22
	▪ Robert Crawhall	<i>Working Together Global Security Scan for Canadian Science Capability</i>	23
3.3	Day 3 – International Perspectives		24
	▪ Mike Corcoran	<i>Changes in Protective Security in the UK</i>	24
	▪ Tony Rutkowski	<i>Protection and Other Mandates for Global Infrastructure: Synergies and Globalization</i>	24
4.	Insights from Day One		25
5.	Working Group Activity		27
5.1	Process		27
5.2	Working Group Reports to Plenary		28
6.	Synthesis		34
6.1	Common Wisdom/Expert Insight		34
6.2	Implications for Future Science Initiatives		34
6.3	Group Wisdom		34
6.4	Individual Insight		37

7.	Conclusion.....	39
	Annex 1 -- List of Participants.....	3
	Annex 2 -- Project Team	5
	Annex 3 -- Workshop Agenda	6
	Annex 4 -- Presentations	7
	<ul style="list-style-type: none"> ▪ Dr. Andrew Valerand <i>Overview of DRDC CSS's Public Security Science and Technology (PSST) Programs and the Importance of FORESIGHT</i> ▪ Shane Roberts <i>Public Safety's Framework: Key Questions and Core Concepts</i> ▪ Jack Smith <i>S & T foresight for Canadian Security and Strategic Preparedness.....</i> ▪ Ken Andrews <i>Global Security Scan for Canadian Science Capabilities (2015-2020)</i> ▪ Steven Featherston <i>Future communications Security Considerations A Telecom, Enterprise and Mobile Infrastructure Perspective</i> ▪ Joseph Decree <i>White Wolf Presentation for the Global Security Scan for Canadian Science Capabilities</i> ▪ Walter Derzko <i>Smart Technologies</i> ▪ Robert Crawhall <i>Working Together Global Security Scan for Canadian Science Capability</i> ▪ Mike Corcoran <i>Changes in Protective Security in the UK</i> ▪ Tony Rutkowski <i>Protection and Other Mandates for Public Infrastructure: Synergies and Globalization</i> 	 7 10 11 14 18 20 31 43 46 50
	Annex 5 -- Working Group Notes	54
	Cyber A – Communications.....	54
	Cyber B – ICT infrastructure for Transport, Finance & Power Distribution	58
	Human Infrastructure 60	
	Physical Infrastructure 65	

Annex 6 -- Additional References	75
<ul style="list-style-type: none"> ▪ <i>Tim Denton Public Safety and National Security Issues, 2015.....</i> ▪ <i>Robert Lesnewich/ Tony Rutkowski, ITU-T Focus Group on Identity Management Report, First Meeting,.....</i> ▪ <i>Geneva, 13-16 February 2007, Implications for NS/EP and CyberSecurity Operational Response</i> ▪ <i>Tony Rutkowski State of ISS February 2007: Principal Developments, Keynote Address – Dubai, Feb. 26-07.....</i> 	 75 79 79 83
Distribution list	86

List of Figures

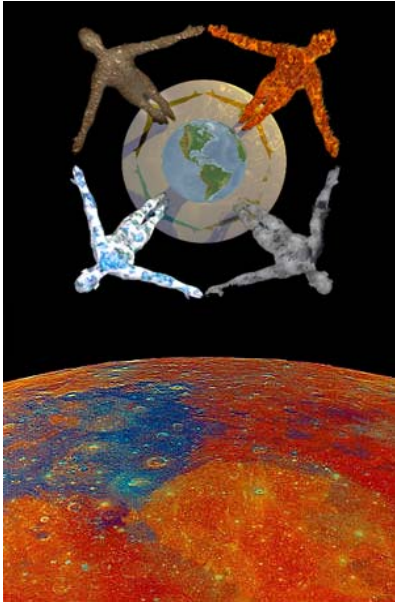
Figure 1	Policy Goals of the Workshop	6
Figure 2	Breadth of the Federal S&T Enterprise	6
Figure 3	New Security Environment: The Drivers	8
Figure 4	Threat & Vulnerability Matrix	9
Figure 5	Critical Sectors: Dependencies on Communications Infrastructure	17
Figure 6	“Intelligence Scale” for Smart Technologies	22
Figure 7	Group Summary S&T Capabilities that are Important & Need Work	36

List of Tables

Table 1	Macro Shaping Trends	8
Table 2	Range of Participant Experience	11
Table 3	Vulnerability Groupings	13
Table 4	Security Matrix – Trends/Gaps and Recommended Focus Areas	18
Table 5	Security Workshop Voting: List of Canada’s Science Capabilities for Security	35
Table 6	Individual Ranking of Science Capability Priority	38

This page intentionally left blank.

1. Foreword



1.1 A Message from the Project Management and Advisory Team

This report represents a summation of the key findings and strategic messages resulting from a foresight security workshop that was designed with two key objectives:

- To review a futures-oriented set of security issues, threats and potential vulnerabilities, so that Canada can design more robust security strategies in the protection of critical infrastructure elements in transport, finance, energy distribution and communications sectors along with their intrinsic cyber capacities,
- To consult with a wide range of security stakeholders about which science and technology (S&T) capabilities will Canada and specifically Defence R&D Canada and Public Safety Canada need to develop, emphasize and deploy, looking ahead to 2015.

This advice is required to support the development of the Public Security Technical Program (PSTP) and its key technical support organization, the new Defence R&D Canada (DRDC) Center for Security Science (CSS). The focus for this aspect of the work has been to enlist a wide range of informed stakeholders to discuss, review and select those S&T capabilities that are believed to be most important to invest in between 2007-2010 so that by 2015 the Center will be fully capable of meeting the key threats and addressing vulnerabilities.

The definition of S&T capabilities remains quite broad, including at least the following:

Alignments of knowledge, intelligence, skills, management, equipment and alliances with other organizations to ensure actionable capabilities by government to act to create and maintain a secure and safe Canadian environment, i.e. both capacity and deployment can be ensured when these are needed.

Addressing Canada's ability to improve its preparedness through foresight and a capabilities analysis will involve consideration of response capacities for many prospective threats, vulnerabilities and readiness contingencies, and that is why foresight is being used to develop a series of responses that are drawn from strategic, stakeholder-driven discussions, and from the consideration of multiple, plausible threat and vulnerability scenarios as best these can be imagined or projected to 2015 and beyond.

The 2007 Workshop was the second attempt to apply foresight methods to the development requirements for the Centre for Security Science. The first assessment of S&T capabilities is detailed in the report: *Security Challenges: Looking Ahead to 2015?* which summarizes the work of the initial workshop held in March 2006.

1.2 Why S&T Foresight?

The Science and Technology Foresight Directorate (STFD) of the Office of the National Science Advisor (ONSA) was asked to advise DRDC and the PSTP on how best to use the foresight approach to identify strategic and operational capabilities pertinent for the security science of the near-term future. STFD produces documents and reports for the benefit of sponsors, participants and professionals interested in how emerging and prospective developments in global science and technology might impact our futures in Canada, North America and the world.

The STFD operates as a collaboratively structured partnership activity within the Canadian Government. Partnerships are developed around specific themes or projects. A range of internationally tested foresight tools and methodologies are employed to stimulate longer-term thinking, develop horizontal linkages and build shared R&D awareness and capacity to better prepare Canadian and global S&T and policy communities for new challenges.

Each project is the property of those who participated in the processes described, and therefore reflects the combined views of the participants and the best wisdom and creative thinking stimulated by the foresight process.

To ensure that this work is not confused with government policy, a disclaimer is regularly applied.

"This work is undertaken under the leadership of the Government of Canada, but does not imply policy, program or regulatory endorsement by its Departments and Agencies unless explicitly indicated.

We regard foresight as contingent research that examines plausible futures that we may have to contend with and as a wise investment in public preparedness."

It is also useful to recall the definition of S&T Foresight that was used to define the scope and focus for this research:

S&T Foresight involves systematic attempts to look into the longer-term future of science and technology, and their potential impacts on society, with a view to identifying the emerging change factors, and the source areas of scientific research and technological development likely to influence change and yield the greatest economic, environmental and social benefits during the next 5 – 25 years.

S&T Foresight is necessarily speculative, creative and analytical.

It relies on both the interpretation of S&T change drivers and on how, if and when these drivers could become significant factors in emerging social, economic and political realities. Since these are highly uncertain, foresight is inherently about attempting to understand and reduce – or at least prepare for – significant risks.

Because of this context of inherent uncertainty, foresight participants and stakeholders should not regard this report as fact or prediction.

It represents collaborative research that was conducted primarily for learning purposes, with the understanding that emerging consensus around some elements might warrant a further, more detailed examination. This is the nature of foresight – creating a range of plausible future scenarios that in their diversity should alert readers to the kinds of issues and perspectives that they may not have considered in initial research planning and contingency thinking.

In foresight, each player, sponsor or participant takes away some collaborative learning and experience that is tacit and more deeply resonant than the descriptive or analytical accounts contained in the reports. These indicate how various foresight approaches and tools can be applied to help readers become better prepared or at least more capable of contingent planning and action in these turbulent times.

We, the four members of the Project Management and Advisory Team bring complementary skills and experience to the foresight process, and we urge you the reader and your organization to also become engaged through this report in the process of determining what new science-based capabilities Canadian security can and should be pursuing up to 2015 and beyond.

Our commitment to this process rests in our belief that foresight brings a very innovative and useful set of new perspectives into the discussion of preparedness, and that is why we urge you to review our findings and contact us if you have questions or suggestions to add to this work.

David McKellar

Senior Advisor, Centre for Security Science

Defence R&D Canada

david.mckellar@drdc-rddc.gc.ca

Shane Roberts

Policy Advisor, Futures & Forecasting

Public Safety Canada

shane.roberts@ps-sp.gc.ca

Robert Crawhall

President and CEO,

National Capital Institute of Telecommunications

crawhall@ncit.ca

Jack Smith

Director, Science & Technology Foresight

Office of the National Science Advisor

smith.jack@ic.gc.ca

2. Context for the 2007 *Global Security Scan for Canadian Science Workshop*

In March, 2006, the *Protective Futures Workshop* was held at the Defence R&D Canada Shirley's Bay facility.³ The workshop was organized to generate foresight that would feed into "Vision 2015" for the Systems Integration, Standards and Analysis (SISA) mission area of the Public Security Technical Program (PSTP) – a joint initiative of Public Safety and DRDC.

Building on the 2006 work, Defence R&D Canada and the Centre for Security Science hosted the *Global Security Scan for Canadian Science Capability Workshop* March 21-23, 2007 at the same Shirley's Bay site.

The 2007 workshop brought together a highly experienced and diverse set of security stakeholders to explore future security issues, threats and vulnerabilities in the transport, finance, energy distribution and communications sectors.

2007 Workshop Objectives

- To review a futures-oriented set of security issues, threats and potential vulnerabilities, so that Canada can design more robust security strategies in the protection of critical infrastructure elements in transport, finance, energy distribution and communications sectors along with their intrinsic cyber capacities,
- To consult with a wide range of security stakeholders about which S&T capabilities will Canada and specifically Defence R&D Canada and Public Safety need to develop, emphasize and deploy, looking ahead to 2015.

2.1 Policy Environment, Conceptual & Methodological Frameworks

Three speakers laid the groundwork for the workshop, providing overviews of the policy environment for security science, of foresight methodology, and conceptual framework used in the public safety analysis.

³ Please see *Security Challenges: Looking Ahead to 2015?* for a summary of this workshop.

Policy Environment

Dr. Andrew Vallerand⁴ situated security and defence initiatives within the complex federal S&T environment, providing an overview of the evolving Centre for Security Science and the process of expanding and broadening the scope of its mission areas.

Participants were challenged to support the project in two ways:

- by contributing to the critical thinking within the workshop event, and
- by identifying and building communities of practice to counteract the limitations of future 'silo' response and research structures.

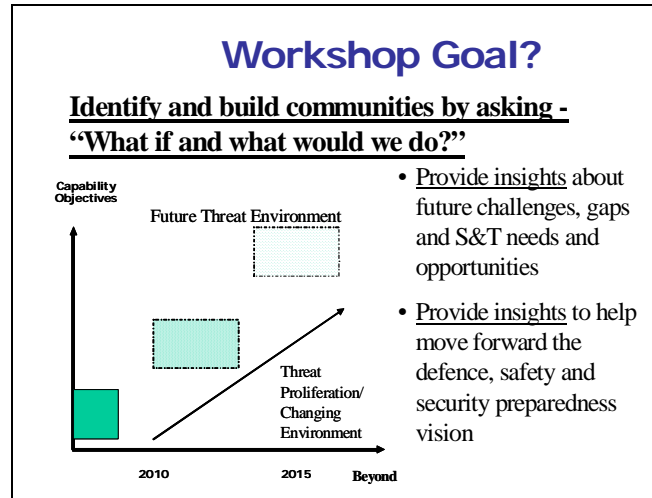


Figure 1
Policy Goals of the Workshop

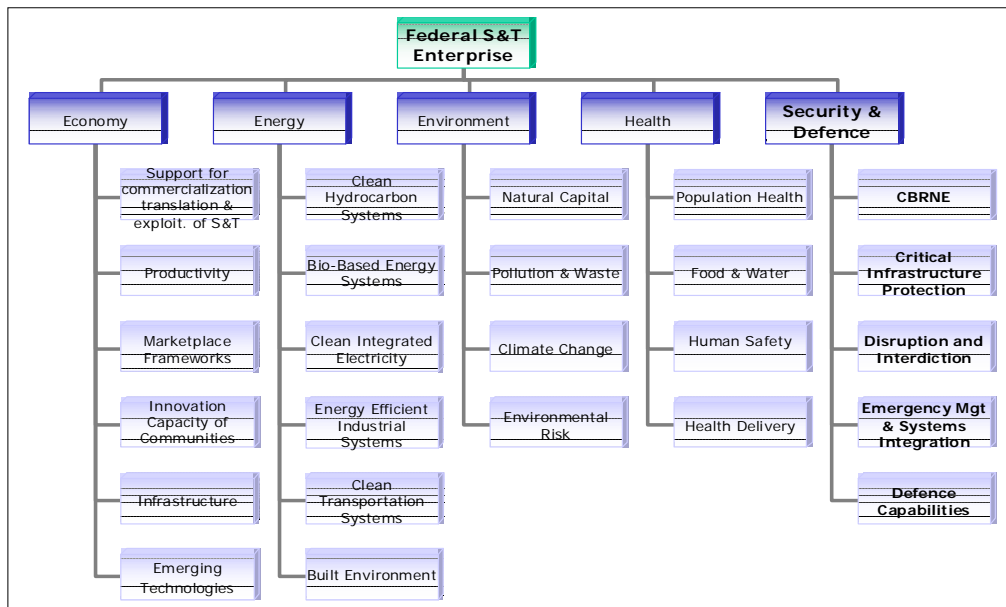


Figure 2
Breadth of the Federal S&T Enterprise

⁴ Dr Andrew Vallerand is the Director, PSTP, DRDC Centre for Security Science. Please see Annex 4 for the full presentation.

Conceptual Framework

Shane Roberts⁵ presented a conceptual framework for the workshop:

Meanings of "Risk"

What are **today's risks** = what risks do we face vis-à-vis critical infrastructure* that could lead to, or compound**, **large-scale emergencies** or compromise public safety and **national security**?

*Telecomms, finance, transportation, energy distribution

** Domino/ripple effect, interdependencies

Constituent elements of Risk:

- **Threats/hazards (natural, accidental, or malicious/terrorism)** & probability of their occurrence
- **Vulnerabilities** (lack of resilience) to the hazards

 Public Safety Canada Sécurité publique Canada

3

The All-Hazards Approach

Threats and hazards

Natural

Extreme weather (rain, ice, drought, wind), forest fires, earthquakes, landslides, solar storms, disease (SARS, AI, Norwalk)

Accidental

Chemical spills (fixed sites, transport), fires, fatigue, faulty ergonomics

Intentional (maliciousness/terrorism):

- Cyber (terrorism, crime, vandal, free-loading business)
- CBRNE, WMDD (Destruction and Disruption)
- Unintentional snowballing & mistakes (youngsters, white powder)

 Public Safety Canada Sécurité publique Canada

4



"Pillars" of Emergency Management

Action (measures) taken to reduce risk (counter threats, decrease vulnerability)

- Pre-event (pre-emergency)
 - Prevention
 - Mitigation
 - Preparation ("preparedness")
- During an event (emergency)
 - Response
- After an event (emergency):
 - Recovery

 Public Safety Canada Sécurité publique Canada

5



⁵ Shane Roberts is a Policy Advisor for Futures and Forecasting with the Science and Technology Policy Division, Emergency Management Policy Directorate, Emergency Management and National Security Branch, Public Safety Canada. For the complete presentation, please see Annex 4.

Methodological Framework: Foresight & Security

A presentation by **Jack Smith**⁶ offered an overview of science and technology foresight methodology and its application in the Canadian context. The presentation focused on security drivers, macro trends and disruptive and enabling S&T – linking them to probable security risks.

Figure 3
New Security Environment: The Drivers

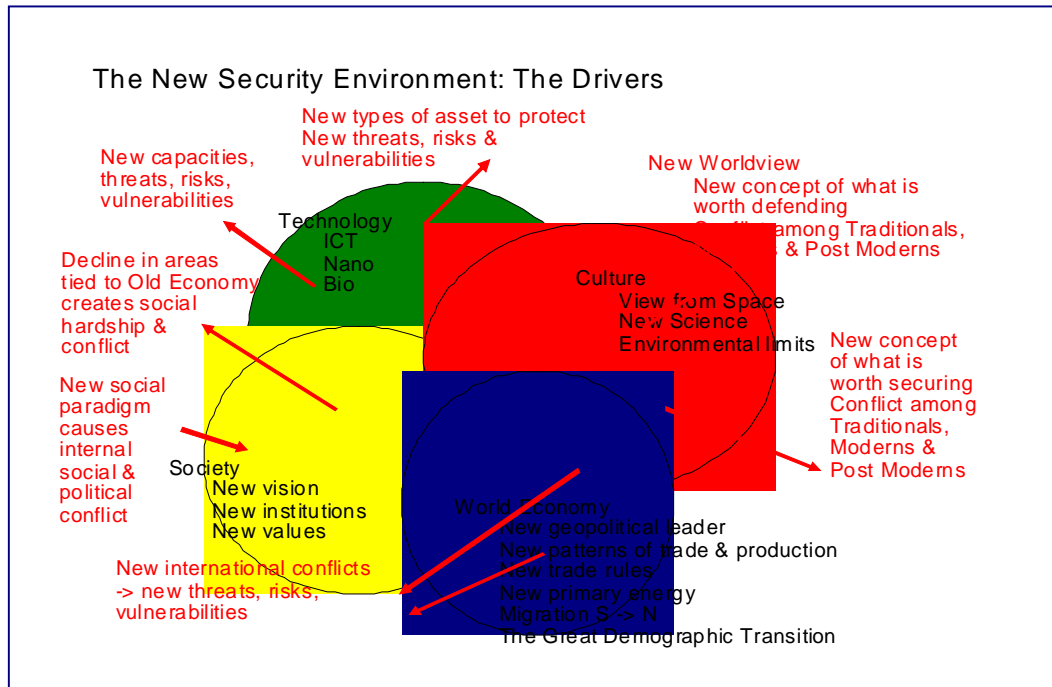


Table 1
Macro Shaping Trends

• Miniaturization of technology	• Globalization/Anti-Globalization
• De-Carbonization, Sustainability	• Harmonization & Standardization
• Transformation of Infrastructure	• Virtualization, Digitization of ICT
• Automated/Customized Production	• Acceleration of Knowledge
• Proliferation of Surveillance	• Asymmetric Conflicts

2.2 Workshop Methodology

The 2006 Workshop and Scan results revealed complex interdependencies and commonalities between and among threats and vulnerabilities across many sectors.

The 2007 Foresight Management & Advisory Team (FMAT) understood from this that these same conditions would apply across all four sectors of critical infrastructure protection (CIP) being examined in 2007 (Figure 4).

At the same time, domain-specific expertise was required to properly identify what areas of S&T could and would be necessary for CIP in the 2015-2020 timeframe and what gaps currently existed in these capabilities both in Canada and globally.

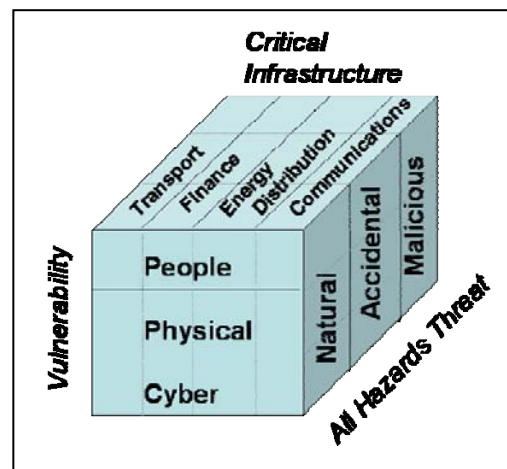


Figure 4
Threat & Vulnerability Matrix

The workshop was structured in four phases:

1) Level setting (half day)

A series of presentations to set clear objectives and rules-of-the-game, establish a common time-horizon, normalize vocabulary across disciplines and stimulate Foresight thinking.

2) Workgroups (full day)

A day of intensive workgroup sessions addressed the S&T requirements and gaps for all-hazards threats each starting from a different lens of vulnerability.

3) International Benchmarking

Invited guests from the US and the UK who had participated in the workgroups provided overviews of international activities and best practices.

4) Synthesis (half day)

Working together using the outcomes from the workgroups the participants generated the list of priorities and recommendations found in this report.

⁶ Jack Smith is the Director of Science and Technology Foresight, Office of the National Science Advisor, Industry Canada. For the complete presentation, please see Annex 4.

Participation Framework

The scan was designed as a workshop rather than a conference. A unique mix of experts from a broad range of disciplines and organizations were asked to work together intensively to seek new and comprehensive insights into the S&T challenges for CIP.

Each participant contributed knowledge and experience as well as expert commentary where necessary. The conclusions were based on open dialog, frank exchange of opinion and the fusing of ideas.

To facilitate openness and knowledge sharing several ground rules were established:

- 1) Participants were present as individuals, selected for their knowledge, experience and skills. Their role was not to represent the positions of their organizations or affiliates. They were requested not to "sell" a particular policy, product, theory or service.
- 2) Individuals would be identified by name, company and whether or not they attended at least one part of the workshop, but no further granularity of participation or attribution would be released except as noted in item (3)
- 3) Individuals who were requested to make formal presentations and opening or closing remarks would be identified and their material would be made available to participants and recipients of the final report.

Participant Skills & Expertise

Fifty-seven individuals drawn from government, industry and academia attended the workshop.

Government participation came from seventeen organizations, a significant but not exhaustive representation of interests closely tied to the CIP process. The wealth of knowledge from the government sector combined with the number of separate organizations involved helped to underline the particular need for the public safety community to provide leadership in tools and techniques for inter-organizational collaboration.

Private sector participation was provided by seven corporations and eight consultants. The individuals present were all experts in S&T, mostly with specialization in security matters. The companies all have active practices across the range of critical infrastructure discussed and brought an international perspective based on direct experience. Several of the companies have significant businesses in areas such as security, transportation and financial systems that are not necessarily well recognized from their name.

Academic participation came largely (although not exclusively) from Ottawa-based institutions due to constraints on time and travel. The nine academics, including people with deep knowledge of two of the major national research funding agencies, all had direct links to programs and research in security and CIP from a wide range of different disciplines.

Table 2
Range of Participant Experience

Academic Disciplines	Government Affiliations	Private Sector
Sociology	National Defence (DND)	Energy Distribution
Political Science	• DRDC	• Canadian Electricity Association
• CIP Policy	Public Health (PHAC)	Communications & Control Equipment
• Security	National Research Council	• Alcatel-Lucent
Electrical Engineering	Industry Canada	Data Systems & Services
• Sensors	Infrastructure Canada	• IBM
• Networks	Office of the National Science Advisor	Communications Services
• Software	Privy Council Office	• Bell Canada
• Robotics	Public Safety	Security Applications
Civil Engineering	• Air Transport (CATSA)	• Third Brigade
• Transportation	• Border Services (CBSA)	• Verisign
• Structures	• RCMP	Security Services
• Earthquakes		• White Wolf Security
• Tsunamis		• Synergy Management
Mathematics		
• Data Mining		

Lenses of Vulnerability

A key challenge for this workshop was to examine in-depth a complex, inter-related set of issues in a compressed period of time. It was clear that there would have to be three or four working groups to achieve an optimal mix of skills and focus.

Three approaches were considered:

1) Analyze by infrastructure

Finance, Transportation, Communications, Energy Distribution

2) Analyze by threat

All-Hazards threats generally consist of a list of between ten and twenty scenarios depending on the source, however, they can be generally grouped as three: Natural, Accidental and Malicious.

3) Analyze by vulnerability

Experience from the 1996 scan exercise indicated that these vulnerabilities had strong cross-sectoral applicability so these were chosen as the lenses through which the workgroups would approach the task at hand recognizing that the other approaches also have their strengths. Experience from the UK wherein the original CIP organizational structure aligned with infrastructure types was later changed to a more vulnerability-based structure.

The vulnerability groupings were essentially defined in Table 3 (below).

Table 3
Vulnerability Groupings

People	<p>People represent a vulnerability for critical infrastructure in two ways:</p> <p><i>Agent of the threat</i></p> <p>They may be the agent of the hazard either intentionally or unintentionally. In terms of S&T this relates to such issues as malicious motivation, authentication and identity management and user interfaces or work practices respectively.</p> <p><i>Victim of the threat</i></p> <p>They may be unable to perform the tasks required to keep the infrastructure operational due to intentional or unintentional health issues – real or potential (e.g. anthrax, chlorine derailment or flu pandemic), civil unrest or terrorism etc. In terms of S&T this relates to biological sciences, epidemiology, technologies and processes for working remotely, automation etc.</p>
Physical	<p>Physical vulnerabilities refer to the ability of physical infrastructure such as buildings, pipelines, transmission towers, pumps, roadways, railways etc. to avoid, resist or recover from threats and hazards. Physical systems may be vulnerable to threats and hazards that are non-physical in nature such as cyber attacks.</p>
Cyber	<p>After extensive discussion the lens of cyber vulnerability was divided into two areas:</p> <p><i>Cyber A</i></p> <p>Dealt with the cyber vulnerability of the public communications infrastructure.</p> <p><i>Cyber B</i></p> <p>Dealt with cyber vulnerability of the domain specific infrastructure for finance, transportation and energy distribution. Each of these CI areas has a strong and growing dependency on the public infrastructure, Internet and NGN (Next Generation Network), however efforts were made not to duplicate discussions in Cyber A.</p>

Selection of Critical Infrastructure (CI) Sectors

The workshop focused on four of the ten areas of critical infrastructure areas identified by Public Safety Canada.

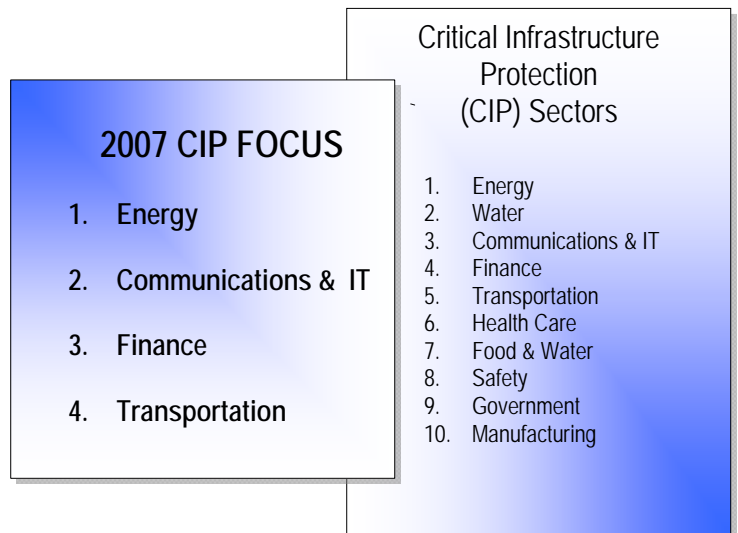
Why were these four areas selected? At the outset it was recognized that addressing all ten critical infrastructure areas (as defined by Public Safety Canada) would not allow the necessary degree of focus needed to obtain useful advice. Addressing only one would fail to identify the high degree of commonality between sectors.

Water, as a vulnerability (as opposed to a threat – too little/too much) was dropped from the original list in order to link it to the food supply in a later session.

Health and government were seen to be large topics – with many specialized concerns – better dealt with separately.

Manufacturing was deemed to be indirectly addressed as energy, transport and communications are major inputs to the integrity of the manufacturing systems.

In addition, concern about the cyber vulnerability of supervisory control and data acquisition (SCADA) systems are common in transportation and energy distribution systems. However, manufacturing as a critical infrastructure has specialized aspects tightly coupled to defence capacity and specific issues around the chemical industry. Many of the recommendations of this report apply to the manufacturing industry, but the participants were not asked to address them directly.



Cyber and Communications

For the purposes of this workshop, a distinction was made between the term *communications* and the term *cyber*.

Communications

Deemed to refer to the public communications service infrastructure including both the physical aspects of that system (equipment, fibre, towers etc.) and the cyber aspects (software, databases, control systems etc.) and human aspects such as maintenance and operations. It is understood that by 2015 the structure of this sector may be significantly different than today. The communications infrastructure, like other critical infrastructures, has vulnerabilities in the people, physical and cyber domains.

Cyber

Defined as the information technology aspects of all critical infrastructure systems. Although not always evident to the casual observer, the efficient operation of all infrastructure systems including transportation and energy distribution is increasingly dependent on information technologies. This trend is expected to accelerate as we approach 2015. CI is vulnerable to the failure of its cyber systems. Threats to the cyber systems may or may not be cyber threats. Regardless of vocabulary used, clarity on these concepts is critical in the shaping of an S&T approach to CIP.

Role of the Social Sciences

A key finding of the 2006 Scan was the need for more focus on the social sciences in the assurance of public safety. This observation has also been made in numerous other forums. S&T strategies often focus on the natural and biological sciences and engineering, areas that have easily quantifiable outcomes. An observation from this process is that significant work needs to be done to understand how social sciences can be incorporated into and S&T framework and their deliverables recognized against appropriate metrics. As previously alluded to the public safety community has particular reasons to take a strong leadership position with respect to incorporating the social sciences in a S&T strategy. Specific efforts were made for this workshop to ensure a balanced representation from the social science sector.

Examples of direct social science contributions are:

- 1) behavioural dynamics between individuals and organizations both under emergency conditions and pre-/post-event are often highlighted as key determinants of outcomes
- 2) cultural, generational and societal factors help explain motivations. Understanding these factors is a major contribution to mitigation of human agent vulnerabilities
- 3) public safety expends significant resources dealing with the public perception of risk (either too high or too low) and the psychological trauma at both individual and societal levels that arise as a consequence of a catastrophic event. Social science contributions can improve the effectiveness and efficiency of these activities

In an interesting corroboration of this point investment in social sciences research to understand societal dynamics was a top priority of the UK CIP program.

3. Stimulus Presentations

Six stimulus presentations were provided prior to in order to get the group thinking about key aspects of the CIP challenge in 2015 – 2020.

The following excerpts provide key concepts and discussion points. The full set of all presentations are provided in Annex 4.

Day 1

Setting the Stage

Stephen Featherston

Future Communications Security Considerations: A Telecom, Enterprise and Mobile Infrastructure Perspective

Joseph Decree

White Wolf Security Presentation

Day 2

Integration

Walter Derzko

Smart Technologies

Robert Crawhall

Working Together

Day 3

International Perspectives

Mike Corcoran

Changes in Protective Security in the UK

Tony Rutkowski

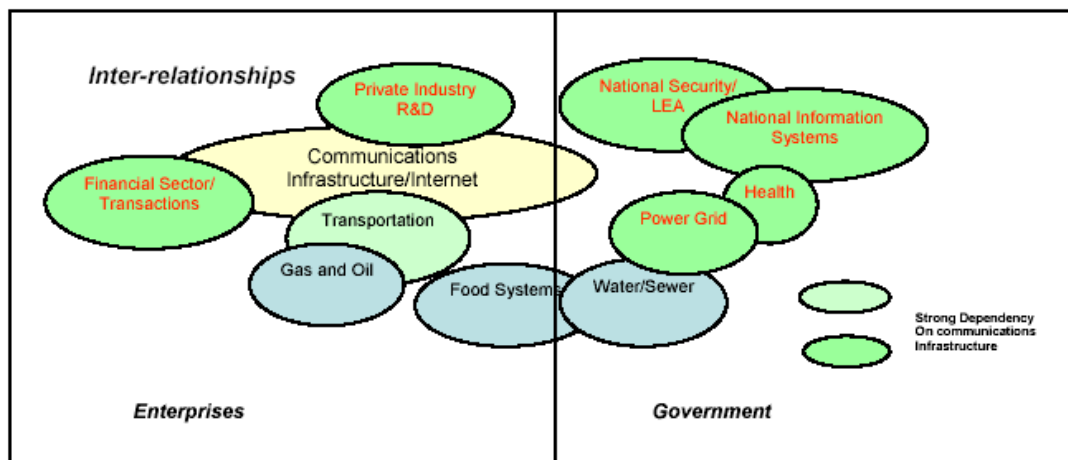
Protection & Other Mandates for Public Infrastructure: Synergies & Globalization

3.1 Day 1 – Setting the Stage

Stephen Featherston⁷ *Future Communications Security Considerations: A Telecom, Enterprise and Mobile Infrastructure Perspective*





Stephen Featherston offered a projection of the telecom and communications sector circa 2015. He posited a world where the economic dominance of India and China would drive more global partnerships dependant on a cost-effective global communications network. Canada's strength, in this scenario, would be based on our R&D and creativity – and the ability to protect our intellectual assets and property. The Internet would be the key delivery system for all voice, data and video transmission and seamless transition between mobile infrastructures will require changes in ownership models. Critical dependencies and vulnerabilities were highlighted.

Figure 5
Critical Sectors: Dependencies on Communications Infrastructure



⁷ Stephen Featherstone is the founder of VOI Solutions, an Ottawa-based telecom and IT consulting firm providing advisory services across a range of practice areas including strategic and tactical business and technology planning; architecture analysis; VoIP security best practices and business continuity planning. www.voi-solutions.ca . Please see Annex 4 for the full presentation.

Table 4
Security Matrix – Trends/Gaps and Recommended Focus Areas

Security Considerations	Cyber	Human	Physical	Trend approaching 2015
Identity Management (“AAA”)	↑	↑	OK	Ubiquitous Strong Authentication will be a requirement because of access to shared multiple apps environment. Also machine to machine authentication.
Crypto Key Management (certify users)	↑	↑	OK	More dependency on services/apps – more emphasis on certification of individual using “any device” from “anywhere”.
Account Management (user id/password mgmt)	↓	↔	OK	Human decisions/monitoring will continue to be critical. (On track). More automation and tools will be available.
Surveillance/Monitoring (identification/prevention)	↑	↔	OK	More need for physical surveillance. New tools will be available for Cyber monitoring. Human factor still required.
Malicious Attacks (intrusion, DOS, Physical security)	↑	↑	↔	Shared applications and inter-enterprise communications will open more doors for cyber based intrusion
Secure Transmission (encryption)	↑	↔	OK	All interactive communications will be encrypted. New “user friendly” techniques with stronger crypto
Back-up/Recovery (BCP’s)	↑	↔	↔	Dependency on shared multiple applications will increase the need for Business Continuity Plans and robust networks and IT infrastructure
Surveillance/Lawful Intercept	↑	↑	OK	Virtual “Anywhere, Any Device” environment adds to challenge
 Increased Focus  Decreased Focus  “Stay the course” Continuous improvement  Existing policies meet requirements				

Key discussion points:

- Q Lots of assumptions in this model – doubtful that three factor authentication will be ubiquitous?
- R Need to find ways to incorporate small authentication in to the device – must be user-friendly.
- Q Heard that IP itself might be outdated, but it may be so firmly entrenched that its inherent vulnerabilities become entrenched as well?
- Q What about delivery models beyond the private sector? San Francisco is offering free WIFI – although the telcos are fighting it. Raises questions on who is delivering the systems...?
- R Telcos will dabble, but cities and others will come into play. Everyone will have to figure out how to do business together.

- Q Challenge the assumption that the physical security issues are resolved. Who will bear the costs? If it isn't resolved... is it a collective action with shared costs?
- R Good question ... we need to be aware – from a critical infrastructure point of view, and might have to do more.
- Q IP infrastructure – most people are saying NGN rather than the term Internet now... signaling will ultimately be the most important element and the challenge will be emulating the IP enabled signaling system...?
- Q Protection of business/government intellectual property – but what about large risk of loss of personal information? There are millions of people who are communicating financial information. How do we protect that information at low enough costs for small business?

Joseph Decree offered a vision for security training based on holistic security model – people, process and technology protecting physical, digital, fiscal and legal assets. He acknowledged that absolute security is unattainable, but remains the goal.

Using military metaphors, he posited every technology worker as a warrior against cyber attacks – “turning every warrior into a sensor”. His 2015 vision – based on current technology trends – called for increasing convergence, ubiquity, mobility and increase in power with decrease in complexity of use. Linked with these trends was an increase in hostile organizations’ use of technology to damage and exploit those they cannot defeat through physical military means.

He pointed to ‘metaverses’ as new tools in cyber terrorism – a new arena for traditional terrorist activity through dead drops for both information and programs, untraceable activities and the potential for the exploitation of cyber economies.

He offered a list of recommendations/tools/ observations to improve security:

Tools & Skills	Notions	Recommendations
<ul style="list-style-type: none"> Tools that reflect the physicality of cyberspace – like Anviss Cross-trained individuals capable of fighting/defending in both the cyber and physical combat spheres Reliable, off-the-shelf defensive/offensive tools Good network design and hourly vigilance Sys-admins need to be warrior-like in their approach to network defence Stay on top of trends & implement policy that supports their effectual & timely use 	<ul style="list-style-type: none"> We can’t un-invent the threat but we don’t have to accept victimization Decentralize the defence process and enlighten the masses Good solid network design Stay abreast of the trends Understand that you are always vulnerable Develop redundancy in critical infrastructure pieces Coordinated kinetic-cyber response 	<ul style="list-style-type: none"> Integrate cyber-space into physical operations NCW is partially about pushing decision-making down to the lowest level and self-synchronization Teach warriors at the small unit level to seek out and exploit network and technological advantages. Turn every warrior into a sensor. Network mapping (wired and wireless) should be as common a task as navigation and personal weapon maintenance.

⁸ Joseph Decree is an instructor with White Wolf Security Systems, a provider of high-end, tailored, hands-on Information Security training based in Lancaster, Pennsylvania. See www.whitewolfsecurity.com. Please see Annex 4 for the full presentation.

Key discussion points:

- Q The concept of asking users of technology to be cyber warriors – it is contrary to what IT shops want – log, log, log...
- R Yes... and teach that person at the desk to meditate and stay physically fit...
- Q Mobile technology, new technology tries to make interface simple to take the human out of computers... so you can't see the pop-ups...
- R Sooner or later you will...
- Q One of the sightlines is that we treat users as if they're dumb, but if you empower them, they get very good at recognizing anomalies, but if they don't think anyone is interested, or they have no way to report it...
- R Most of us are associative learners – the easiest person to teach to be a hacker or network defender is a combat arms infantryman – because it's attack and defend...
- Q Reference to the Chinese – availability of government facilities to general hackers. And to Russian organized crime – do the ROC have access to any government equipment?
- R Don't know, but suspect it's probably not necessary...
- Q Observation – having more technology – people tend to trust it – number of times I get documents that have been thru spellchecker – culture is not to do due diligence...
- R Agreed.
- Q Contentious security model of VISTA – constantly popping up – something has been requested, accept or deny? Appears to involve user more in security process... but the result is that people go into auto-accept...
- R That's *your* problem. Focus.
- Q You are putting a heavy requirement on the user – how many of the people here actually read the accept requirements from websites before accepting? The average person has no clue what those mean... so what's the point?
- R Network design should be better... if we made it so that they only popped up when NECESSARY... then people would pay attention. Empower people further – demystify the networks, etc. But give them the right level of info and tools...

3.2 Day 2 – Integration

Walter Derzko ⁹

Smart Technologies

This wide-ranging presentation on smart technologies provided a very brief overview of the range of smart technologies currently and soon to be in production. “Smart Technologies” – both systems and objects – were defined as machines or artifacts that do something we think an intelligent person can do.

Figure 6
“Intelligence Scale” for Smart Technologies



Intelligence Level (1)	Adapting:	Modifying Behavior to Fit the Environment	
Intelligence Level (2)	Sensing:	Bringing Awareness to Everyday Things	
Intelligence Level (3)	Inferring:	Drawing Conclusions from Rules and Observations	
Intelligence Level (4)	Learning:	Using Experience to Improve Performance	
Intelligence Level (5)	Anticipating:	Thinking and Reasoning about What to Do Next	
Intelligence Level (6)	Self-creating,	Able to reproduce itself	
Intelligence Level (6)	Self-organizing	Ability for components to self-organize	
Intelligence Level (6)	Self-sustaining (A)	Ability to replicate components	
Intelligence Level (6)	Self-sustaining (B)	Ability to process information	
Intelligence Level (6)	Self-sustaining (C)	Ability to steadily consume energy from the environment	

© 2005-2006 Walter Derzko Walter Derzko; The Smart Economy Blog
Toronto, Canada 416-533-9667

⁹ Walter Derzko is a Toronto-based futurist and business development consultant interested in strategic planning and thinking, futures research, emerging smart technologies, scenario planning, issues management, environmental scanning, opportunity recognition and lateral thinking. See *The Smart Economy* <http://smarteconomy.typepad.com>

Smart Technology Design Exercise

Participants were invited to take part in an exercise to conceptualize new positive and negative applications from a set of artifacts, or technologies identified at random.

The audience identified three artifacts/technologies – “working variables”:

1. Spray or print on electronics
2. Self assembly & dis-assembly
3. Synthetic porphyrins – power source from photosynthesis

From these, participants ‘created’ positive and negative potential applications:

Positive applications	Negative applications
<ul style="list-style-type: none">• Self-reproducing 3-D printer – solar-powered – drop 1 into a village in central Africa and entire continent becomes a self-enabled industrial power• Wireless home electronics• Camping satellite TV	<ul style="list-style-type: none">• Bomb with spray on electronics that will assemble and dis-assemble• Spray on an ATM that could change and get info from user – sun powered• Same thing as a threat to North America• Kills manufacturing/retail chain – revolution• Redistribute economic power – cottage industry – don’t need cities• Spray on motion detector for military/police• Secure supply train – build sensor into packaging

Robert Crawhall ¹⁰

Working Together
Global Security Scan for Canadian Science Capability

Robert Crawhall shared experience from his work with the National Capital Institute for Telecommunications (NCIT) – bringing together “multi-disciplinary, multi-party, collaborative research involving the private sector, academic and government labs...”. He urged participants to look beyond the specific jargon of their discipline and take the time to understand meaning rather than recite acronyms. The value of the session is on finding the common understanding of the workgroup informed by the individual expertise of the participants.

¹⁰ Robert Crawhall is president of the Ottawa-based National Capital Institute for Telecommunications and a member of the Project Team for this workshop. Please see Annex 4 for the full presentation. For more information on NCIT, visit www.NCIT.ca.

3.3 Day 3 – International Perspectives

International perspectives were provided after the working group meetings and before the plenary group set to work on the combined recommendations. Please refer to Annex 4 for the full presentations.

Mike Corcoran

Changes in Protective Security in the UK

The first presentation was provided by Mike Corcoran of the UK Centre for Protection of National Infrastructure regarding the CPNI mandate and S&T priorities and best practices. The UK has been dealing with terrorist threats for over thirty years and has recently gone through major emergencies such as mad cow disease.

This workshop was not designed as a best practices session and the UK presentation was unclassified and informational, however, it was very instructive to see that the working group summaries aligned well with the priorities as described in the UK process.

Tony Rutkowski

Protection and Other Mandates for Global Infrastructure: Synergies and Globalization

The second presentation came from the Vice President of regulatory affairs from Verisign, a leading provider of on-line information security services. Although based in the US and reflective of current US trends in on-line security issues, the presentation dealt principally with international trends and the standards initiatives to counter cyber threats.

This presentation pointed out a major global trend to apply targeted regulation to communications services such as obligations to save routing information as a way to track child predators, obligatory security standards for work on government projects, identity management initiatives and the emerging use of third-party identification certificates such as CardSpace. Two messages came from this presentation:

- 1) Governments are taking a leading role in evolving the communications infrastructure to mitigate cyber threats.
- 2) Canada appears to be lagging other jurisdictions such as Europe, the Far East and the US in pursuing regulatory mechanisms against cyber threats.

4. Insights from Day One

The workshop organizing team recognized that the impact of the range of information and discussion from Day One would have provided participants with much food for thought. An effort was made to gather participant comments and ideas prior to moving into the working group activities. This allowed organizers and participants to benefit from early collective wisdom, and also gave participants a chance to become engaged.

Summary of Participants' Comments

- Most interesting – Joe's presentation – everyone needs to be a sensor, trained. My experience is that information technology policy isn't about empowering users but about making them obedient – so this seems completely antithetical to security – we need to include the citizen in the discussion about security – empowering them...
- Not sure yesterday we all understood what security really means – we need a definition – including understanding what the public understands is a safe and secure environment – start state and end state... transportation and energy probably okay – what are the risks to the other sectors... need to look at the vulnerabilities...
- Looking at threats from terrorists, governments, criminals & hackers – all with different reasons, and targets – intentional hazards...
- Organizer interjects – today we'll look at natural and then look at intentional – it's an all hazards perspective...
- Add another to the list – "unintended screw-ups" – couple of years ago – a poor Microsoft patch created huge problems – drove queries back to the server... there is more of this type of thing than we realize. In cyber-security there are ubiquitous new platforms – e.g. Vista – will take user through every potential security threat – then on a continuing basis ensures that security will be maintained – but ultimately infrastructure based security mechanisms – government provided...
- But how about Vista "user fatigue" for security...?
- See a lot of incidental sources of media exaggeration of fear...leads to bad decision-making...
- Centre won't be doing anything about laws, but there is a good report from European Union... on S&T needs – recommends that projects be awarded based on many variables including human considerations (includes ethics and justice)...
- 2 additional factors – 1) business model – incentives – and also 2) risk perception... interesting to study how people perceive risks and how you can change perceptions...
- Been to four sessions on this and now pleased to see that the "human factor" is being incorporated...when you talk about risk it has to do with human action/decision-making... leading to behaviour modification. Our science has a human factor built in ... we invent

technologies in our own image... would like to see more emphasis on human, social side of things...

- Everything we are talking about – human, cyber, physical is about defence term for information operations (IO) – influencing your adversaries to obtain advantage...
- Need to define security – but also need to realize what we are protecting... conflict between security and freedom – open society – can't protect and destroy what we are protecting. We can embed rules in technology so we protect what we want... important as law becomes embedded in software...
- How critical is setting the context for security deployment, measures, attitudes – understanding we're dealing with cyber attacks – so have to be warriors... be alert to signals, sources, technology is a double-edged sword – human centred factors are important – trust, reliability...
- Risk may be too "soft" a word – risk is not all bad – risk adverse companies don't grow. Maybe need to look at attacks and counterattacks..... play down the term risk a bit...
- Seeing a dichotomy in the 1995 AG report on the difficulty in the relationship between partnering and accountability in a government context – knowledge management... decoupling allows alternate technologies... a contradiction... if you know what you know and have the best info it tends to lead to centralization – which makes you more vulnerable...
- Feeling constrained by needed science deliverables – think about gasoline affected by refinery fires... one by BP in the US traced back to a corporate cost-cutting measures – consequences flow, and yet security affected ... is there a scientific issue? A business model? Let's not be so constrained by the deliverable that we miss important conditions. Look at the school shootings... science wouldn't have helped. Let's avoid silos...
- Define the terms... what is risk, what does security mean to Canada. Is it on-line porn or a terrorist attack? Define the term then define the most heinous thing that can happen... and focus...
- Complicated issue – what is knowable and who knows it – and what is not knowable – look at insurance companies – develop histories of systemic, equipment and other failures. History of components... knowledge is power in competitive markets, accountability... so private sector doesn't share because it invests and knowledge keeps the owner healthy. But if you do a historical accounting... if you keep records long enough you will find that extraordinary things do occasionally happen – but you can't plan business for that. When you have fundamental shifts ... you can throw out the historic records... big worry for insurance business. Modeling has lots of possibilities but it may be knocking public on its fear... treatment of risk. We can't tell them what the risk is...

5. Working Group Activity

5.1 Process

Participants self-selected one of four working groups for a full day of intensive exploration of the S&T requirements and gaps for all-hazards threats.

Four breakout teams:

1. Cyber A
2. Cyber B
3. Human Infrastructure
4. Physical Infrastructure

Cyber A focused on the Communications Sector.

Breakout Teams

Team Name	Focus 'Lens'	Comms. Sector (telecoms, networks, responders)	Transport Sector (air, rail, marine, surface)	Finance Sector (banks, TSX)	Energy Distrib. (power lines, oil/gas pipelines)
Cyber (A)	Inform'n, IT, nets, s/ware, h/ware	☯			
Cyber(B)			☯	☯	☯
Human Infra.	People, workers, decisions	1st	☯	☯	☯
Physical Infra	Plant, buildings, cities	1st	☯	☯	☯

Cyber B focused on the other three sectors.

Human & Physical focused first on the communications sector, and then sought elements unique to the other three sectors.

Breakout Questions

1. What are the most critical threats and vulnerabilities looking at your sector through your lens (in 2020)?
2. What are the responses* in the ideal world?
3. How could science support/enhance these responses*?
4. What science must be started now (2007), to be ready in 2015-2020?
5. What S&T capabilities** are therefore needed in Canada?
6. Any unique differences for the other sectors (if applicable)?
7. Prepare 'synthesis' page for team – key points & insights

Each team answered several questions....

"Responses" & "Capabilities**"*

Timing

before event

during event

after event

Action

prevention/mitigation/preparation

response

recovery/learning

...and considered *the timing/action* issues linked to each response and capability.

"Science Capabilities": knowledge, intelligence, skills, equipment, tools, networks, alliances ...

5.2 Working Group Reports to Plenary

In an attempt to create an immediate synthesis for participants, working groups were asked to report back question by question. The first group outlined their findings for each question, and the second, third and fourth followed – highlighting key additions or differences. At the end of the four reports for each question, the audience was asked to identify common themes that appeared across sector reports.

A more elaborate capture of the working group data is contained in Annex 5 – Working Group Notes.

1. Most critical threats & vulnerabilities

Cyber A

- Outsourcing of software development – for mission-critical systems... threat is malicious code
- Meshed sensor networks ... security, integrity, availability
- Ubiquitous networks inherently complex – no one knows how to secure – identify management
- Humans as a vulnerability – threat social engineering
- Increased physical threats –
- Increase in cyber warfare – don't have to go anywhere – DND, PS and others, coordination required and tools computer network operations, CAN, CNE, etc
- Identity becoming more important, passports etc. human – machine and vice versa... identity theft

Cyber B

- What did cyber mean?
- Transport – cyber makes things move more securely,
- Finance – cyber – now a cyber business – some interfaces between physical and cyber world of finance
- Energy – very cyber dependent
- All systems will be greatly cyber dependant, but threat will be exponentially worse than now – will change whole dynamic of security – it will be much bigger than our current defensive posture
- Much greater complexity and interdependency...
- Wild weather and other things will create greater demands
- Border security – will require huge databases –systems become more brittle - ...
- Trend...number of attacks will increase massively – growing knowledge gap – good guys and bad guys... easier to find a vulnerability than to build a secure system
- Nation or multi-national attacks
- Asymmetric attacks – small bits of code create massive disruption

Human

- Modern civilization – key words
- Microbial diseases
- Drivers:
 - Global mobility – spreads disease
 - International – number of people with advanced degrees
 - Increasing specialization of people, orgs, lead to need for greater redundancy
 - Rigid occupational structures – globally movement of people, goods, pathogens but organizations too rigid
 - Demographic shift – dependency ratio, human capital loss, lack of foreign credential recognition
 - Cross border issues with USA
 - Urbanization and democratization –
 - Currency control
 - Violent jihadist extremist – first nations, environmentalists, anti-globalists, militant farmers, youth, immigrants, labour strife

Physical

- Energy distribution has ripple effect to everything
- Key threats destruction of physical infrastructure, denial of access, cascade effect, extreme weather – more frequent
- Transportation – vulnerability is jurisdictional cracks
- Energy – permafrost melting, higher reliance on cyber

Common Themes

- Impact of Kyoto... greater energy use combined with reduced capacity...Chindia coming on-stream...unless nuclear is greatly increases – there will be an energy shortage
- Ripple effect, complexity, interdependency
- Dysfunctional jurisdictions
- Distributed governance – international and domestic
- More angry people who want to inflict damage on complex systems
- Space-time compression – greater access, quicker access, greater damage

2. Actions and responses

Cyber A

- Awareness, better planning, coordination,
- Deal with different motivations from public-private owners of various systems
- Better collaboration
- New first responders profiling and org development
- Proactive national security infrastructure

- Mathematics capability for expert modeling for complexity – for detailed issues – algorithms for human behaviour and institutional behaviour
- Quantifiable differential levels of trust – better complexity – will require math and system integration
- Regularizing activities for activities for simulation, modeling
- Better redundancy
- New IP protocols with enhanced security related to differential levels of trust
- National warning and authenticity systems through meshed networking
- More secure protocol on the Internet
- Incident strategies
- First responders knowledge management systems

Cyber B

- Control network for SCADA system?
- Identification of vulnerabilities way behind
- Computer science stuff around databases – maybe government systems will pull through and private sector may have abandoned. May no longer be capacity to pursue
- Self-healing systems
- Current attacks different from 2015 attacks
- Strategies for red-teaming

Human

- Assured representation at international bodies in standards, protocols and trade
- Collaboration, communication, breaking down silos
- Joint management activity requires some shared consciousness – not only moving information but need same lexicons... embedded cultural values... different ways of understanding how things run... organizational cultures, subcultures... collaboration
- Game theory, complexity, modeling – developing services and systems to support – need to get beyond pitfalls of small group interaction – augmented cognition...
- Emphasis on getting to know people through exercises – man/machine exercises, getting players to work together and understand their foibles

Physical

- Threat 1 – systemic interconnectivity and cascade affect – before, during, after event
 - Better modeling ahead of time, systems management
 - Practice responses
 - Apply learnings to improve models
 - Good early warning systems
 - Common operating picture amongst different sectors
 - During event – fast response – automated
 - Data logging during events
 - Lessons learned
 - Business resumption plan
- Threat 2 – explosions, the destruction of infrastructure

- Before – better surveillance, detection, modeling
- Make target harder – physically and through distribution, etc.
- During – faster response
- After – identify culprit, find, rectify, or resolve him

Common Themes

- Modeling
- Quantify trust
- Inter-organizational coordination
- Exercises, drills, lessons learned

3. What science would support or enhance these actions & responses?

Cyber A

- GENERIC – capability to detect malicious code and revise
- R&D for security and sensor networks – how they operate, transmit
- Capacity to deal with ad hoc network security
- Modeling of human motivations
- Inventory of physical networks and their interconnectedness with cyber exposure...
- What needs protection & what's exposed
- Capability to invest in preventative measures
- Capability in identity management, authorization
- Capabilities...
 - Algorithmic development for trust and authentication behaviours
 - Map critical system assets
 - Deal with a business/government service model with interactive management capacities

Cyber B

- Modeling – self-defending systems, skater vulnerability detection technology,

Human

- Augmented collaboration – inter-jurisdictional, organizational – designing tools for teams, organizations, other social groups, etc... collaborative activity
- Augmented cognition – threat identification, weeding through vast data sets, helping people think
- Skill sets that would help:
 - Cultural/ social anthropology
 - Operations research
 - Cognitive psychology
 - Epidemiologists

- Sociologists
- Data mining
- Rapid vaccine development

Physical

- Mathematics – essential for protecting
- Psychology – how to implement lessons learned, crisis management, perceptual, etc.
- Complexity science
- Earth sciences – geophysics
- Material science and architecture – smart materials, etc.

Common Themes

- Modeling & mathematics
- Complexity science
- Augmented collaboration
- Understanding human nature
- Engineering – combination of science and engineering
- Better communications between people – clearer info exchange

4. What science needs to be started now to be ready in 2020? What science capabilities are needed in Canada?

Most of it!

Cyber A

- Inventory of physical connectivity link
- Malicious code
- Algorithmic trust, identify
- Capability for institutional inter-connectivity

Cyber B

- How does Canada get a place at the table where other nations are investing?
- Identify those areas of science where we could leverage our current assets to get to those tables.

Human

- Anything related to exercises, drilling, technology to enhance it
- Harnessing human capital – make better use of newcomers to Canadian society

Physical

- All

5. Synthesis – Key Insights and Conclusions

Cyber A

- Critically detect intruders
- Identity management
- Human vulnerabilities
- Offensive mechanisms
- Inventory
- Malicious detection

Cyber B

- Now actions – improved warnings
- Incremental improvements to network security
- Improved analysis of risk and survivability
- Increased collaboration and improved information intelligence – inter-jurisdictional, industry, academy
- How to create right communities of practice and associations of people... take the ten critical infrastructures and create nodes on transportation etc.
- Vincent leading an initiative to create a community of practice for cyber-security

Human

- What characterizes contemporary society – specialization – but in a crisis how do you cut across this specialization in a timely basis – peer production? Also exploitation and management of human capital

Physical

- Recognizing that not every threat is intentional or malicious
- Physical infrastructures for a complex – necessity for holistic security ecosystems approach
- Security strategies resilient
- Physical infrastructure is disappearing
- Importance of foresight and scenario evaluations – epidemiology
- Technology will have more interaction with and be more intelligent re the environment
- Need for low tech in a future high tech world
- Science solutions must accommodate combinations of natural and accidental threats...

Common Themes

- Communities of practice
- Epidemiology

6. Synthesis

6.1 Common Wisdom/Expert Insight

An unusual aspect of this working group was that the final exercise of consolidating and prioritizing recommendations and insights from the four working groups was done in a full plenary session. Care was taken to ensure that the participants, experts from a wide range of disciplines, understood the terminology and concepts involved in the consolidated list of priorities. Those who had specific expertise in each area were asked to provide some background on why these were relevant and finally to give some indication of whether this was a field with significant current activity.

Following the review the participants were asked to rate (as opposed to rank) the list of S&T capabilities against three criteria:

- 1) did they feel they had sufficient knowledge to pass judgment
- 2) did they think it was important
- 3) if important, did they think it was being taken care of sufficiently or was it a gap that needed addressing.

This activity resulted in the consolidated recommendation list below.

Next the participants were asked to rank the three most important items (including items that did not make the list) based on their expertise and the discussion of the past two days. This activity resulted in the second set of recommendations.

6.2 Implications for Future Science Initiatives

Organizers and participants felt that the methodological framework described above was a good tool for analysing a complex set of interdependencies and arriving at recommendations that reflected the understanding of the group while respecting the expertise of the individuals. It is recommended that this framework be considered when creating the future plan of work.

6.3 Group Wisdom

Following the methodology outlined above, the workshop participants identified the following list of Science Capabilities for Security through the four working groups. In the plenary discussion that followed they each indicated their opinions both of the importance of the item in building competencies for CIP in the 2015-2020 timeframe and the degree to which they felt that the item was already being dealt with. Individuals were not asked to rank the items in terms of importance at this point of the process. If an item is both "Important" and "Well Taken Care Of" then it is the general advice of the working group that CSS ensure that the responsible parties are aware of the work. If an item is

"Important" but "Not Well Taken Care Of", then the advice is to foster development of the areas of inquiry through partnership and capacity building.

Table 5
Security Workshop Voting:
List of Canada's Science Capabilities for Security

<i>Capability Descriptor *</i>	<i>Important</i>		<i>Not Really Important</i>	<i>Offered Knowledge/Opinion</i>
	<i>Not Well Taken Care Of</i>	<i>Well Taken Care Of</i>		
Self-Healing Cyber Systems	91%	9%	0%	69%
Inter- and Cross-Cultural Collaboration	90%	10%	0%	91%
Human Motivation, Cultural Anthropology & Operations Research	87%	13%	0%	91%
Inter-Organizational/ Augmented Collaboration, Cognition and Ergonomics	87%	10%	3%	91%
Complexity Science; Viable Systems Modeling	81%	19%	0%	76%
Infrastructure Planning & Redundancy Theory	80%	17%	3%	88%
Offensive Cyber	72%	20%	8%	74%
Simulation, Modeling, Foresight	70%	27%	3%	94%
Software Assurance, Malicious Code Detection & Code Reverse Engineering	70%	30%	0%	68%
Workforce Vulnerability to an Attack	63%	33%	3%	88%
Algorithmic Trust Quantification	62%	21%	17%	85%
Network Epidemiology; Dynamics of Networks	60%	36%	4%	74%
SCADA Security	54%	46%	0%	76%
Risk Analysis	47%	50%	3%	91%
Crisis Behaviour Management	46%	50%	4%	76%
Smart Materials	40%	53%	7%	88%
Sensor System Design: Testing, Prediction, Warning	7%	60%	3%	88%
Practices, Drills & Preparedness Exercises	33%	67%	0%	88%
Data Fusion and Data Mining	32%	58%	10%	88%
Cyber Intrusion Detection	21%	79%	0%	97%
Climate Physical Infrastructure Impacts	19%	61%	19%	91%
Encryption	3%	91%	6%	97%

Figure 7 shows a graphical ranking of the top eleven items from Table 5 based on the percentage of “Important and needs work”. Judgment must be used in interpreting the precise ranking however, if 90% of the individuals who were comfortable passing judgment believe that it is important and not being taken care of that is a clear indication that something should be done.

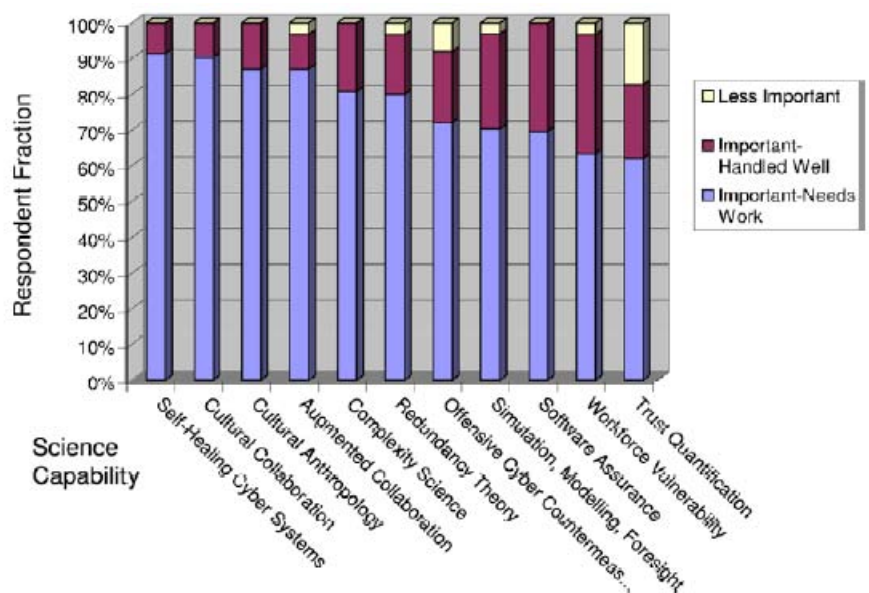
Similarly, in the case of encryption 94% believe it to be important but 91% think there is sufficient effort already in place that item can be removed from the gap analysis.

Figure 7
Group Summary S&T Capabilities that are Important & Need Work

The eleven items in Figure 7 represent a broad but balanced view of capacity building requirements.

Four are technical in nature:

- Self-Healing Networks - the ability for cyber infrastructure to recover quickly and elegantly from cyber threats.
- Offensive Cyber Measures – the capability to “push back” on cyber malfeasance from individuals, organizations and states.
- Software Assurance – automatic procedures and formal methods to verify that software systems are doing what you want them to do and no more.
- Trust Quantification – the process of knowing how much to trust persons or things in cyberspace.



Two are tools to facilitate the smooth functioning of CIP systems:

- Augmented Collaboration – tools to facilitate and mediate collaboration across organizational, cultural or geographic barriers.
- Simulation, Modeling & Foresight – the ability to exercise “what-if” scenarios.

Four are social science/operations research areas:

- Cultural Collaboration – studies in how various social groups interact
- Cultural Anthropology – studies in the understanding of various social groups
- Redundancy Theory – how we partition work and layout physical infrastructure to allow for redundancy in the face of both unintentional and intentional threats. (Most current theory is focused on random, unintentional threats and provide little redundancy to a malicious disruption)
- Workforce Vulnerability – a combination of epidemiology and work-systems research to quantify the exposure of critical infrastructure operational integrity to loss of workforce due to people vulnerabilities.

Finally, Complexity Science is a multidisciplinary field that spans mathematics, systems theory and cognition. Taken as a bottom-up exercise, critical infrastructure protections systems are complex and indeterminate. Approached theoretically practical and tractable solutions may be found. Complexity is generally a poor indicator of reliability and survivability. Complexity specifications from software to transportation systems can mitigate the effects of all-hazards threats.

6.4 Individual Insight

Following the group analysis the individual experts were asked to select and rank their top three priorities. When reviewing the ranking it is important to emphasize that there areas for which expert knowledge was fairly well represented and others where one person alone understood the problem in depth. Also the participants were asked which they thought were the most important rather than which they felt were gaps. By combining the results of the group and individual rankings some insights can be gained into importance and gap analysis.

Table 6
Individual Ranking of Science Capability Priority

Rank	Science Capability	Score
1	Inter-Organizational/Augmented Collaboration, Cognition and Ergonomics	13.4%
2	Complexity Science; Viable Systems Modeling	12.0%
3	Simulation, Modeling, Foresight	9.9%
4	Infrastructure Planning & Redundancy Theory	8.7%
5	Practices, Drills & Preparedness Exercises	7.2%
6	Human Motivation, Cultural Anthropology & Operations Research	5.9%
6	Self-Healing Cyber Systems	5.8%
8	Risk Analysis	5.4%
9	Inter- and Cross-Cultural Collaboration	4.7%
9	Crisis Behaviour and Management	4.3%
11	Algorithmic Trust Quantification	3.6%
11	SCADA Security	3.0%
11	Network Epidemiology; Dynamics of Networks	2.9%
14	Data Fusion and Data Mining	2.5%
15	Workforce Vulnerability to an Attack	2.1%
15	Cyber Intrusion Detection	1.9%
17	Climate Physical Infrastructure Impacts	1.7%
17	Offensive Cyber Countermeasures	1.6%
19	Sensor System Design: Testing, Prediction, Warning	1.3%
19	Software Assurance, Malicious Code Detection & Code Reverse Engineering	1.2%
21	Smart Materials	0.7%
22	Encryption	0.0%

Some of the areas that appear in the upper half of the individual analysis that were not in the top of the group analysis are:

- 1) Ergonomics for the reduction of human error.
- 2) Practices, drills and preparedness exercises
- 3) Security of supervisory control and data acquisition systems

7. Conclusion

The three-day workshop yielded a number of clear recommendations for the development of science-based capabilities for the security and protection of critical infrastructure in Canada. The core recommendations apply quite consistently across the four areas of critical infrastructure that were investigated and are expected to have application to the other six areas. Many of the activities discussed have already been done or are in the process of being done amongst Canada's allies. Partnerships are expected to be an important element of capacity-building.

The threat environment in 2015-2020 will be significantly harsher than today. Investments in security science will be essential to meeting the challenge. In terms of time to develop new knowledge and deploy it in practical applications 2015 is not far away. Work must start now on the areas of highest priority.

Annexes

Annex 1	List of Participants
Annex 2	Project Team
Annex 3	Workshop Agenda
Annex 4	Presentations
Annex 5	Working Group Notes
Annex 6	Additional Reference Material

Annex 1 -- List of Participants

Kenneth Andrews	High Impact Facilitation
Ray Baldwin	Industry Canada
Gwen Beauchemin	Public Safety Canada
Cam Boulet	DRDC Ottawa
Francis Bradley	Canadian Electricity Association
Ronald Bragdon	DND
Thomas Brzustowski	University of Ottawa
Nick Cartwright	Transport Canada
Paul Chouinard	DRDC
Stanley Chow	Alcatel-Lucent
Steffen Christensen	Consultant
Michael Corcoran	Centre for Protection of National Infrastructure
Robert Crawhall	NCIT
Joseph Decree	White Wolf Security
Tim Denton	Consultant
Walter Derzko	The Smart Economy
George Emery	National Research Council
Steve Featherston	Voice Over Internet Solutions
Gregory Fyffe	Privy Council Office
Gary Glavin	Public Health Agency of Canada
Abd el Halim	Carleton University
David Harries	Royal Military College of Canada
David Hidson	Consultant
Valerie Howe	Justice Canada
Diane Keller	Canada Border Service Agency
Marc Lafleur	Bell Canada
David Lau	Carleton University

Julie Lefebvre	DRDC
Peter MacKinnon	Synergy Technology Management & and National Security Infrastructure Partnership
Paul McCullough	IBM
David McKellar	DRDC
Craig McNaughton	SSHRC
Shirley Mills	Carleton University
Brian O'Higgins	Third Brigade
David Peter	RCMP Technical Crime Branch
Emil Petriu	University of Ottawa
Shane Roberts	Public Safety Canada
Dane Rowlands	NPSIA
Tony Rutkowski	Verisign
Murat Saatcioglu	University of Ottawa
Mark Salter	University of Ottawa
Abhijit Sarkar	Carleton University
Karl Schroeder	Thalienne Communications
Jack Smith	ONSA
Lynelle Spring	Springworks Consulting
Brian Staples	Consultant
Harold Stocker	DRDC
Vince Taylor	DRDC
Jean Thie	Canadian Institute of Geomatics
Mihaela Ulieru	University of New Brunswick
Andrew Vallerand	DRDC
John Verdon	DND
Jennifer Wozny	Privy Council Office

Annex 2 -- Project Team

Ken Andrews	High Impact Facilitation k.j.andrews@rogers.com
Robert Crawhall	National Capital Institute of Telecommunications crawhall@ncit.ca
David McKellar	Defence R&D Canada, Centre for Security Science David.mckellar@ddrc-rddc.gc.ca
Shane Roberts	Public Safety Canada shane.roberts@ps.gc.ca
Jack Smith	Office of the National Science Advisor, S&T Foresight smith.jack@ic.gc.ca
Lynelle Spring	SpringWorks Consulting lynellespring@rogers.com

Annex 3 -- Workshop Agenda

Global Security Scan for Canadian Science Capabilities (2015-2020)

Agenda

Wednesday, March 21

- | | |
|--------------|--|
| 11:00 – 1:00 | Registration |
| 1:00 – 5:00 | Welcome, objectives, meeting format
Introduction to Centre for Security Science

Stimulus Presentations: Security Scan; Communications Challenges;
Mobile Infrastructure; Tracking in Cyberspace |

Thursday, March 22

- | | |
|--------------|---|
| 8:00 – 9:00 | Breakfast |
| 9:00 – 12:00 | Insights from Day #1
Overview of Foresight and Security Science

Breakout teams to consider responses in selected sectors in 2015-2020:
a) critical threats and vulnerabilities
b) ideal responses
c) science and technology (S&T) to support these responses
d) S&T capabilities required by Canada |
| 12:00 – 1:00 | Lunch |
| 1:00 – 5:00 | Breakout teams (contd.)
Report to plenary, discussion & synthesis |
| Evening | Workshop dinner |

Friday, March 23

- | | |
|--------------|--|
| 8:00 – 9:00 | Breakfast |
| 9:00 – 12:30 | Stimulus presentations

Breakout teams: prioritize S&T capabilities for CSS

Report to plenary, discussion & synthesis
Next steps & close |

Annex 4 -- Presentations

Dr. Andrew Valerand *Overview of DRDC CSS's Public Security Science and Technology (PSST) Programs and the Importance of FORESIGHT*

Canada

Overview of DRDC CSS's
Public Security Science and
Technology (PSST) Programs and
the importance of FORESIGHT

Dr. Andrew L. VALLERAND

Director PSTP
DRDC Centre for Security Science
Mar 07

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 1

Canada

Agenda

- 1 Overview of the context today
- 2 PSS&T Overview
- 3 PSTP Overview
- 4 Importance of FORESIGHT
- 5 Questions, comments, survey...

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 2

Canada

DELIVER Safety & Security in a changing world: a complex Security & Defence challenge!



Canadian Border
1/2 Mile Ahead

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 3

Canada

The Issue: Is Canada Prepared?

- New, complex and emerging threats require forward-looking, scientific and technical solutions.
- Investment in S&T solutions can advance Canada's security capabilities to prepare for and prevent short and long-term, natural and human-made security threats and disasters.

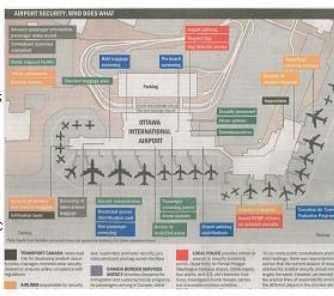


DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 4

Canada

A Recent Example: Airport Security

- The front page article in the January 20th Ottawa Citizen featured airport security.
- Several federal agencies and private sector concerns are involved in airport security.
- The article spoke to a lack of interoperability amongst the numerous security organisations.
- This is an example of public security which presents both challenges and opportunities to the public and private sectors.



DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 5

Canada

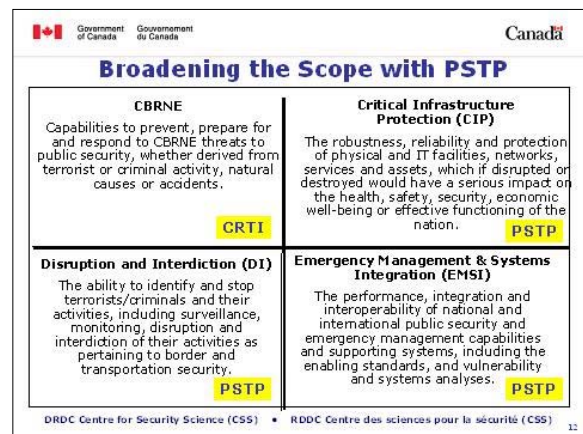
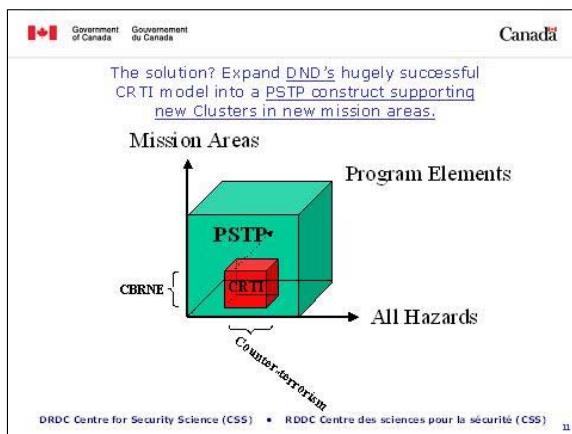
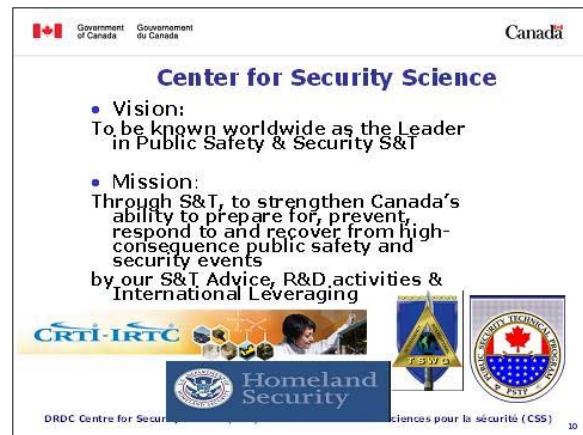
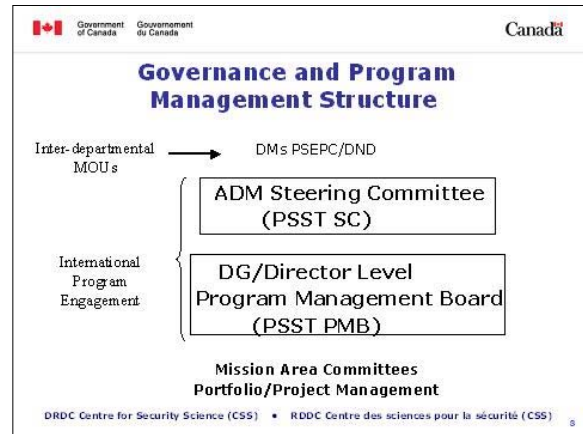
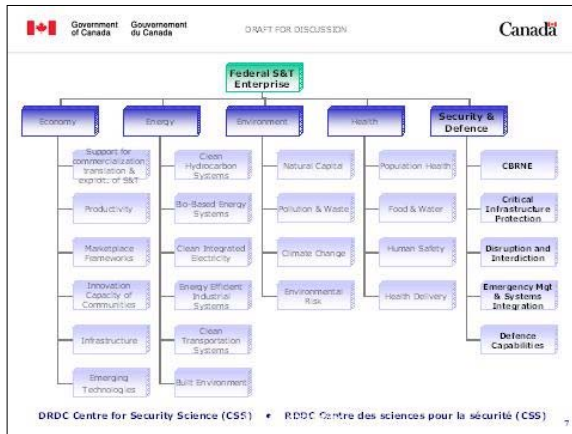
The Context Today

- Continued interest in the National Security Agenda
- ADMs Science Integration Board - Federal S&T Enterprise
- Industry Canada led Federal S&T Strategy
- Recently released Defence S&T Strategy

Emerging complex events continue to pose a significant risk to Canada and Canadians

Canadian Public Security Science and Technology Strategy

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 6



Government of Canada / Gouvernement du Canada Canada

DRDC Centre for Security Science

- Created by Departments of Public Safety and National Defence – **MOU DND/PSEPC**, signed August 2006
- Coordinates the federal public S&T Strategy and the resulting S&T program with a range of federal partners including academic and industrial networks
- Coordinates S&T reach-back into the federal S&T community including DRDC, NRC, NRCAN, PHAC, CFIA, RCMP, etc.....
- Funds Exercises/Workshops for Responder community
- Integral part of Defence S&T program with links to Canada Command
- Coordinates International Activities: **MOU DHS S&T**

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 13

Government of Canada / Gouvernement du Canada Canada

Public Security S&T Mission Areas

CBRNE (CRTI)

- Chemical
- Biological
- Radiological/Nuclear
- Explosives
- Forensics

Critical Infrastructure Protection (CIP)

- Physical CIP
- Cyber CIP
- Energy, Comms & IT; Finance; Health care; Food & Water; Transport; Safety; Government; Manufacturing; including the interdependencies

Disruption & Interdiction (DI)

- Intelligence and Surveillance
- Policing and officer safety
- Border D&I
- Transportation D&I
- Maritime D&I

Emergency Management & Systems Integration


- Risk Assessment, Foresight
- Emergency Response & Recovery
- Interoperability Framework
- Modelling & Simulation
- Standards, Tech forecast
- Psycho-Social Factors
- Search and Rescue

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 14

Government of Canada / Gouvernement du Canada Canada

EMSI Studies

- At the outset, the PSTP identified the requirement for several key fundamental studies:
 - Vision 2015**
 - Risk Assessment Methodology**
 - Interoperability
 - Decision Support

 • The Vision 2015 is the cornerstone that guides future capability needs

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 15

Government of Canada / Gouvernement du Canada Canada

Vision 2015 and Risk Assessment

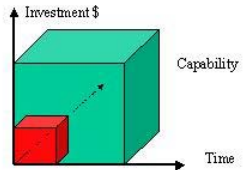
- Initially, these two studies are being delivered in parallel and are mutually supportive
- Risk Assessment currently deals with current and near term gaps
- Objective is to anticipate future gaps and position S&T investments
- The Vision piece will establish the capability targets

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 16

Government of Canada / Gouvernement du Canada Canada

Current Risk Assessment

- Deals with the near term threat
- Needs to be informed to consider mid to longer term risks
- Must inform future capability objectives
- Should guide investments towards future capabilities



Capability

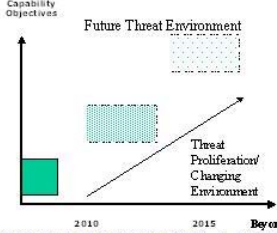
The assumption is that the threat is proliferating faster than counter-measures are implemented

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 17

Government of Canada / Gouvernement du Canada Canada

Workshop Goal?

Identify and build communities by asking - "What if and what would we do?"



- Provide insights about future challenges, gaps and S&T needs and opportunities
- Provide insights to help move forward the defence, safety and security preparedness vision

DRDC Centre for Security Science (CSS) • RDDC Centre des sciences pour la sécurité (CSS) 18

Public Safety's Framework: Key Questions and Core Concepts

Global Security Scan for Canadian Science Capabilities
(Ottawa, 21 March 2007)

Shane Roberts - Policy Advisor for Futures and Forecasting
Science and Technology Policy Division
Emergency Management Policy Directorate
Emergency Management and National Security Branch
Public Safety Canada

Key Questions for the Near Term

How Public Safety Canada frames its approach
**emergency management (EM) and
the protection of critical infrastructure (CIP)**

- Looking at the *current environment*:
"What are **today's risks**, and
what **capabilities** do we need to meet them?"
- Looking to our R&D partner, the Centre for Security
Science: "How can S&T contribute to **currently
needed capabilities**?"

Meanings of "Risk"

What are **today's risks** = what risks do we face vis-à-vis
critical infrastructure* that could lead to, or compound**,
large-scale emergencies or compromise public safety
and **national security**?"

*Telecomms, finance, transportation, energy distribution

** Domino/ripple effect, interdependencies

Constituent elements of Risk:

- **Threats/hazards (natural, accidental, or
malicious/terrorism)** & probability of their occurrence
- **Vulnerabilities** (lack of resilience) to the hazards

The All-Hazards Approach

Threats and hazards

Natural

Extreme weather (rain, ice, drought, wind), forest fires, earthquakes,
landslides, solar storms, disease (SARS, AI, Norwalk)

Accidental

Chemical spills (fixed sites, transport), fires, fatigue, faulty
ergonomics

Intentional (maliciousness/terrorism):

- Cyber (terrorism, crime, vandal, free-loading business)
- CBRNE, WMDD (Destruction and Disruption)
- Unintentional snowballing & mistakes (youngsters, white powder)

"Pillars" of Emergency Management

**Action (measures) taken to reduce risk
(counter threats, decrease vulnerability)**

- Pre-event (pre-emergency)
 - Prevention
 - Mitigation
 - Preparation ("preparedness")
- During an event (emergency)
 - Response
- After an event (emergency):
 - Recovery

How you can help

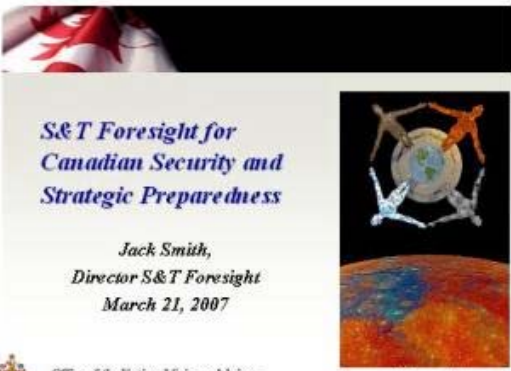
Extend Public Safety's vision over a longer time-frame

"The near term" – a necessary but incomplete focus

- **Today's risks** and **currently needed capabilities**?"

"Over the horizon" – anticipating and preparing

- Thinking about **risk over the long term**: "What is happening in
the world and how is it changing the profile of risk – i.e. the
threats & vulnerabilities of tomorrow?"
- PS and CSS: "What are the **capabilities we need for tomorrow**
and for which work should start today?"



S&T Foresight for Canadian Security and Strategic Preparedness

Jack Smith,
Director S&T Foresight
March 21, 2007

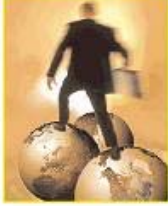
Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

What is Foresight?

A set of strategic tools that support government and industry decisions with adequate lead time for societal preparation and strategic response.

- Anticipates multiple, plausible futures
- 5 – 25 year time horizon
- Are rehearsal or potential futures
- Accommodate uncertainty & diversity
- Highlights emerging opportunities & threats



Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Foresight Tools

- Environmental Scanning
- Scenario Planning
- Technology Mapping and Road-mapping
- Expert Technical Panels
- Robust Factor Analysis
- Web Virtual Conferences
- Computerized Modelling and Dynamic Simulation



No trouble the greatest map, nor we can't figure out how to find it?

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

ONSA Foresight 2004 - 06

Canadian Foresight – ONSA Led

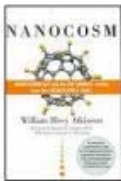
Challenges	Results
• Future fuel technology options, alternatives to conventional oil	• Technology roadmaps for bio-fuels, hydrogen fuel cells, unconventional hydrocarbons
• Technology innovation for the Canadian Health System	• Technology maps and health commercialization advice, identified new technologies and regulatory stewardship
• S&T for public safety and all hazards Canadian security	• Threat scenarios, S&T strategies for the DND-C – PERSC Center for Security Science, links with US DHS, British Critical Thinking On c.
• How to manage public attitudes to nuclear fusion and mass waste disposal	• Technology communication exercises for the CFTA to manage R&D and threats to public health, and strategies for proactive public uncertainty reduction
• How bio-product might factor into our future economy	• Scenario and Canadian policy drivers for emerging bio-product markets and development paths

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Environmental Scanning

- **Strategic Trends:** i.e. factors that shift as a result of change patterns, but we have little influence. e.g. more nuclear equipped nations; failing states proliferation;
- **Critical Drivers and Uncertainties:** i.e. discernible change patterns that may be amenable to stakeholder actions; e.g. global security, major S&T developments
- **Possible Shocks:** i.e. wild card, high impact, low probability events that alter fundamentals; e.g. 9-11; Iran as a nuclear power




Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Environmental Scanning

To identify the emergent, characterize prospective disruptors, dimension the unfamiliar, and track the potentially high impact domains, causal actors.

1. Description: signal type – domain, character & relevance
2. Critical Linkages & Interdependencies
3. Time Line: projection to 2010, expectation 2015; speculation 2025
4. Vulnerability: risk and probability factors for Canada
5. Canadian science & technology impacts, discontinuities, and capabilities-opportunities for leadership
6. What if this factor goes in the opposite direction?
7. Key knowledge management references
8. Policy research elements and questions-options



Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

New Security Drivers

Technology
Society
Culture
World Economy

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

New Security Drivers

The New Security Environment: The Drivers

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Brockman's List : The Next 50 Years

1. Cyberspace as information beams, portable teleconnection & ubiquitous smart networks;
2. Bio-engineering of bio-robotics, artificial life models;
3. Quantum math & computing, teleportation, computational and emergent complexity;
4. Search for ETI and biophilic universes;
5. Neuro-science & convergent cognition, computational pharmacology, neuro-regeneration;
6. Subterranean rheumatology & Triphibious flexible transport;
7. Nano-structural products, sensors, materials, fabrication and molecular tailoring.

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Fraunhofer-Germany List

1. Smart Environments – micro components, smart sensors, cyber-logic;
2. Adm-Machine Corporation – intuitive brain-computer links;
3. Polymers – plastics in display, energy systems and virtual environments;
4. Digital Medicine – imaging, simulations, medications via genomics, proteomics;
5. Digital Logistics – automated commerce – transactions, storage, fleets;
6. Augmented Production – digital mass customized and virtual, flexible products;
7. Adaptive Structures – piezo-ceramics to change vibration, noise, save energy;
8. Photonics BioNet – universal light controls: medicine, electronics, materials;
9. Nano-Cryo-Print – extreme ultraviolet nano-printing resolution, applications;
10. Simulation and Modelling – of everything – quantum & real computing power;
11. Customized Energy – distributed, portable networks, low central power.

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Macro Shaping Trends

- Miniaturization of Technology
- Globalization-Anti-Globalization
- De-Carbonization, Sustainability
- Harmonization and Standardization
- Transformation of Infrastructure
- Virtualization, Digitization of ICT
- Automated-Customized Production
- Acceleration of Knowledge
- Proliferation of Surveillance
- Asymmetric Conflicts

SCIENCE AND TECHNOLOGY FORESIGHT
NIC-CNIC

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

Disruptive, Enabling S&T

Personalized Genomics
Neuro-Cognitive Brain
Nanotechnology
Quantum Computing
Internet 2020

Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada

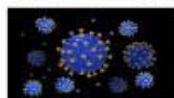
Foresight for Security: a New Challenge

- Foresight enables diverse security contexts, threats and societal factors to be simulated and examined within the context of turbulence;
- The Security challenge and response capacity are both rapidly evolving in concert with technological capacity;
- S&T evolution is likely to be disruptive and may revolutionize present security dynamics;
- Creating robust research, training and security personnel response strategies need to be an essential outcome from S&T foresight;
- The security context for all hazards is also very interdependent with ecological and human factor stress levels and rehearsal-readiness mindsets – foresight can support and amplify institutional readiness.



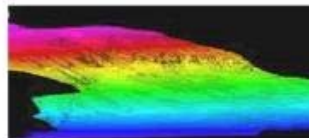
Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada



What New or Enhanced Capabilities Will be Needed?

1. Security focused foresight processes;
2. Research into how S&T can mitigate all hazards and deal with new threats, critical infrastructure, emergent, convergent & disruptive technologies;
3. R&D and Responder Training Models;
4. Continuous Technology Assessment - Mapping;
5. Expert Consultation Networks – who and how;
6. Regular fora for sharing intelligence, foresight with US, UK, other allies



Canada



What are the Likely Public Safety & Security Risks?

- Too much technological - S&T self reliance
- Limited international collaboration
- Permitting fast depletion of renewable resources - environmental burden, overload
- Global warming? 'inevitable surprises'
- Natural and all hazards intensify



- Lack of 'surge capacity' response
- Need for a Arctic strategy-capacity for threat intervention
- Environmental refugees
- Infrastructure disruption
- Terrorism in Canada



Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada



How Can S&T Help?

- Human Systems & Personality Modelling
- Integrative Threat Modelling
- Nanoscale Detection
- Neuro-cognitive Science
- Genetic Modelling & Prediction
- Pervasive Sensor Networks
- Robotics & Surveillance-Intercession
- Cyber & Quantum Security
- Critical Infrastructure Protection



Office of the National Science Advisor
Bureau du Conseiller national des sciences

Canada





*Global Security Scan
for
Canadian Science Capabilities
(2015-2020)*

Ottawa
March 21-23, 2007

Confidentiality

- ✦ Meeting of experts: provide personal perspective (not corporate)
- ✦ Nothing will be attributed (recordings wiped after meeting)
- ✦ Your name & organization only will be listed in the report
- ✦ Nothing classified please



Meeting Agenda: March 21 (Day #1)

- 11:00 – 1:00 Registration
- 1:00 – 5:00 Welcome, Introductions & Objectives
- Meeting Format & Agenda
- Introduction to Centre for Security Science (CSS)
- Stimulus Presentations: Public Safety Framework:
Security Scan
Communications Challenges
Mobile Infrastructure
Tracking in Cyberspace
- Plenary Discussion

Meeting Agenda: March 22 (Day #2)

- 9:00 – 12:00 Insights from Day #1
Overview of Foresight and Security Science
Perspectives on 'Working Together'
- Breakout teams to consider responses in selected sectors in 2015-2020:
- a) critical threats and vulnerabilities
 - b) ideal responses
 - c) science and technology (S&T) to support these responses
 - d) S&T capabilities required by Canada
- 12:00 – 1:00 Lunch
- 1:00 – 5:00 Breakout teams (contd.)
Report to plenary, discussion & synthesis
- 6:00pm Workshop Dinner

Meeting Agenda: March 23 (Day #3)

- 9:00 – 12:30 Stimulus presentations
- Plenary discussion on status of S&T capabilities
- Personal perspectives on priorities capabilities for the Centre for Security Science
- Next steps & close

Objective/Deliverables

To identify for the Centre for Security Science the most critical science-based capabilities to anticipate and respond to all hazards to Canadian security in four critical areas:

- ✦ Communications (e.g. telecoms, networks, responders)
- ✦ Transportation (e.g. air, rail, marine, surface)
- ✦ Finance (e.g. banking, TSX)
- ✦ Energy distribution (e.g. transmission, oil & gas pipelines)



Breakout Teams

Team Name	Focus 'Lens'	Comms. Sector (telecoms, networks, responders)	Transport Sector (air, rail, marine, surface)	Finance Sector (banks, TSX)	Energy Distrib. (power lines, oil/gas pipelines)
Cyber (A)	Inform'n, IT, nets, s/ware, h/ware	☯			
Cyber(B)			☯	☯	☯
Human Infra.	People, workers, decisions	1st	☯	☯	☯
Physical Infra	Plant, buildings, cities	1st	☯	☯	☯

Page 20



Global Security Scan for Canadian Science Capabilities (2015-2020)

Welcome to Day #2

Ottawa
March 21-23, 2007

Page 21

Meeting Agenda: March 22 (Day #2)

- 9:00 – 12:00 **Insights from Day #1**
Overview of Foresight and Security Science Perspectives on 'Working Together'
- Breakout teams to consider responses in selected sectors in 2015-2020:
- critical threats and vulnerabilities
 - ideal responses
 - science and technology (S&T) to support these responses
 - S&T capabilities required by Canada
- 12:00 – 1:00 **Lunch**
- 1:00 – 5:00 **Breakout teams (contd.)**
Report to plenary, discussion & synthesis
- 6:00pm **Workshop Dinner**

Page 22

Sector Breakout Teams – Step #1

- Select a Sector by picking a Post-It from the appropriate wall-chart ('limited seating')
- Proceed to your breakout area, with your Facilitators
- Review & clarify the foci for your team: sector(s) and lens
- Read the breakout questions – clarify if necessary
- Brainstorm and capture responses to Question #1; identify the most critical bullets
- Repeat the process for Questions #2 - #6
- At the conclusion, review your responses, and capture your team's most interesting insights & conclusions
- Prepare to share your ideas in plenary at 2:30pm in Auditorium (take lunch at noon)



Page 23

Breakout Teams

Team Name	Focus 'Lens'	Comms. Sector (telecoms, networks, responders)	Transport Sector (air, rail, marine, surface)	Finance Sector (banks, TSX)	Energy Distrib. (power lines, oil/gas pipelines)
Cyber (A)	Inform'n, IT, nets, s/ware, h/ware	☯			
Cyber(B)			☯	☯	☯
Human Infra.	People, workers, decisions	1st	☯	☯	☯
Physical Infra	Plant, buildings, cities	1st	☯	☯	☯

Page 24

Breakout Questions

- What are the most critical threats and vulnerabilities looking at your sector through your lens (in 2020)?
- What are the responses* in the ideal world?
- How could science support/enhance these responses*?
- What science must be started now (2007), to be ready in 2015-2020?
- What S&T capabilities** are therefore needed in Canada?
- Any unique differences for the other sectors (if applicable)?
- Prepare 'synthesis' page for team – key points & insights

Page 25

“Responses*” & “Capabilities**”

Timing	Action
before event	prevention/mitigation/preparation
during event	response
after event	recovery/learning

“Science Capabilities”: knowledge, intelligence, skills, equipment, tools, networks, alliances ...

For 55

24

Team Notes

- ◆ This is a brainstorm – there are no ‘right’ or ‘wrong’ answers
- ◆ Try to help your facilitator, by providing short bullet responses
- ◆ Consider the questions through your ‘lens’, only for your sector(s) (e.g. lens = physical infrastructure) (e.g. sector = communications)
- ◆ Think in the context of the 2020 timeframe (i.e. NOT today)
- ◆ Keep in mind a Canadian perspective, not global
- ◆ Remember that we are to conclude with science capabilities; don’t be concerned about differentiating science from technology
- ◆ Consider all hazards and vulnerabilities: natural, accidental & intentional/criminal/terrorist

For 55

25

Sectors & Facilitators & Location

Focus Lens	Process Facilitator	Technical Facilitator	Location
Cyber (A)*	Jack Smith	Walter Derzko	Rm 223, Bldg 74
Cyber (B)**	David McKellar	Robert Crawhall	Conf. A, Bldg 5
Human Infrastructure	Shane Roberts	Karl Schroeder	Rm 224, Bldg 74
Physical Infrastructure	Ken Andrews	Steffan Christensen	Auditorium

* Communications sector only

** Transportation, Finance & Energy Distribution sectors only

For 55

26

Global Security Scan for Canadian Science Capabilities (2015-2020)

Welcome to Day #3

Ottawa
March 21-23, 2007



For 55

27

Meeting Agenda: March 23 (Day #3)

- 9:00 – 12:30 Stimulus presentations
- Plenary discussion on status of S&T capabilities
- Personal perspectives on priorities capabilities for the Centre for Security Science
- Next steps & close

For 55

28

Objective/Deliverables

To identify for CSS the most critical science-based capabilities to anticipate and respond to all hazards to Canadian security in four critical areas:

- ◆ Communications (e.g. telecoms, networks, responders)
- ◆ Transportation (e.g. air, rail, marine, surface)
- ◆ Finance (e.g. banking, TSX)
- ◆ Energy distribution (e.g. transmission, oil & gas pipelines)



For 55


29

Plenary Discussion: Science Capabilities

1. Handout of synthesized list of science capabilities from Day #2
2. Plenary discussion of item #1 – sharing expert information & knowledge from the participant group
3. Then all participants may 'vote' on his/her personal list

Page 43

Personal Science-Capability Table

#	Science Capability Descriptor	IMPORTANT		NOT REALLY IMPORTANT	NO OPINION
		Being taken care of	NOT being taken care of		
1					
2					
3					
4					
5					
6					
7					

Page 44

Plenary Discussion: Science Capabilities

1. Handout of synthesized list of science capabilities from Day #2
2. Plenary discussion of item #1 – sharing expert information & knowledge from the participant group
3. Then all participants may 'vote' on his/her personal list
4. Repeat the steps 2 & 3 for all listed capabilities
5. All lists are collected and collated (during break)
6. Review composite list in plenary
7. Every participant prepares a personal "Top-3 Science Capabilities for CSS" (these will be provided to facilitators, at the end of workshop)
8. Participants are invited to share & discuss their list in plenary (if they wish)

Page 45

Personal Science-Capability Table

#	Science Capability Descriptor	IMPORTANT		NOT REALLY IMPORTANT	NO OPINION
		Being taken care of	NOT being taken care of		
1		6	27	4	14
2					
3					
4					
5					
6					
7					


Page 46

My Personal Recommendations for the Top Priorities for the Centre for Security Science

#	Science Capability Descriptor
1	
2	
3	
Other Comments	

Page 47

Steven Featherston *Future communications Security Considerations* *A Telecom, Enterprise and Mobile Infrastructure Perspective*




Future Communications Security Considerations

A Telecom, Enterprise and Mobile Infrastructure Perspective

Steven Featherston
VOI Solutions
613-837-7131
sfeatherston@voi-solutions.ca
www.voi-solutions.ca

1



Objective and Outline

Presentation Objective:

- Address the future security of the Canadian Communications Infrastructure with a focus on:
 - future mobile environment
 - evolution of Telecom and Enterprise communication networks and services
- Flag potential future security risk areas which maybe outside of the current policy environment.

Presentation Outline:

- Assumptions - "The world in 2015"
- Future communications environment and vulnerabilities
- Inter-relationships of Critical Infrastructure Areas and potential communication based applications.
- Security Matrix and potential detailed threat assessment
- Summary - Suggested focus areas for conference

2




"The World in 2015" – Economic and Political Assumptions

- India and China will dominate the world economy
 - Partnerships and mergers will be key for Canadian companies to compete in the Global economy
 - Cost effective Global communications key to ensure Canada's competitive edge
 - Strong R&D presence and protection of Canadian Intellectual Property key to ensure Global competitive advantage.
 - Protection of assets and secure infrastructure
- Terrorism will still be a threat
 - New vulnerabilities will emerge based on Western Societies societal behaviors and use of new technologies
- We will be at some level of war or conflict

Business, Academia and Governments will need to partner to ensure Canada's Economic Success

Need to provide our Security Services, Military and LEA's with the tools to protect our Nation


3




"The World in 2015" – Technical Assumptions and Definitions

- The Internet will become "THE" method of transport for all voice, data & video transmission and collaboration.
- The definition of Mobility will change.
 - Today – most North American's think of Cellular services (cell phone, BlackBerry).
 - Tomorrow – Mobility defined as individuals moving seamlessly between various broadband accesses on any device, with a full suite of services, any time, anywhere.
- Society will depend heavily on broadband accesses and the Internet, driven by new higher bandwidth applications/services
 - Individuals
 - Business
 - Government
- "Net head" and "Telco head" philosophies will merge, to a degree, creating shared 3rd party applications and a more open "Net-neutrality" environment.
 - Business and Governments will use trusted Internet based applications

4



Future Network Environment – Convergence of Networks



Network Convergence

- Separate networks evolving to converged architecture
 - Shared applications from any broadband access using a common, IP based Switching network
- IP will be the Primary medium for voice (VoIP). Public Switched Telephony Network (PSTN) will be "dying" in 2015
- Software driven "intelligent" IP devices

Infrastructure


- Cellular 3G (384 Kbps – 2 Mbps)
- Wireless 4G (WiMax) "Ethernet speed"
- Fibre to the home/business – 100's of Mb/s
- Core IP Network (transitioning to IP-V6) with "soft-switching"

Crossing Boundaries

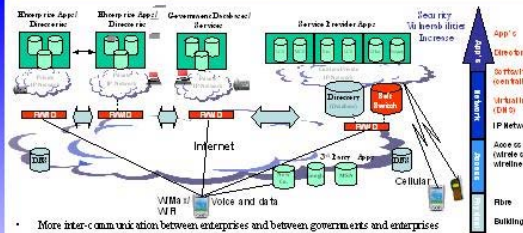
- Seamless crossing of various Mobile infrastructures, owned by multiple companies/institutions
- Same user experience regardless of device or access type (wireless or wireline)
- Increased interaction between "network centric" carrier based services/applications and Private Enterprise directories and apps.
- More Enterprise to Enterprise communications.

Security is usually an afterthought when developing new network technologies and protocols

5

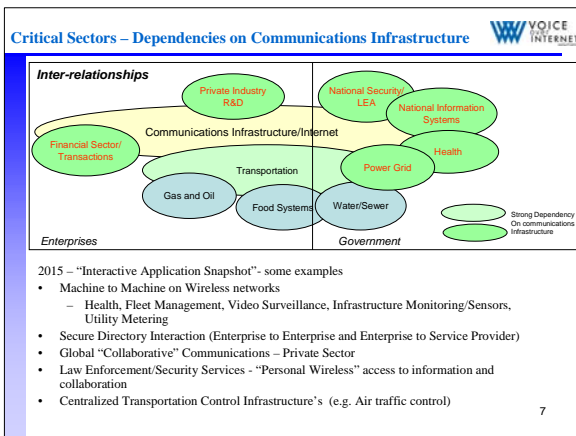


Future Network Environment – User Experience and Key Infrastructure Vulnerabilities



- More inter-communication between enterprises and between governments and enterprises
- Hybrid environment of web based (less secure) and service provider (more secure) Services and capabilities.
 - Presented to user as one integrated experience (e.g. Single user interface)
- Network moving towards centralized architecture (failure has greater impact)
- High Level Vulnerabilities – Communications Infrastructure
 - Physical Infrastructure – OK
 - Access/wireless – limited impact due to distributed nature
 - Soft-switching/DNS – failure could have national or global impact.
 - Applications/Directories – failure could have national or global impact. Complex Environment.

6



Framework for Discussion – A Security Matrix based on ISO Standards (ISO 17799)

Security Considerations	Cyber	Human	Physical
Identity Management (Authentication)			
Crypto Key Management (certify users)			
Account Management (user id/password mgmt)			
Surveillance/Monitoring (identification/prevention)			
Malicious Attacks (intrusion, DOS, Physical security)			
Secure Transmission (encryption)			
Back-up/Recovery (BCP’s)			
Surveillance/Lawful Intercept			

- Used for IT Security Governance (Best Practices)
 - Considers Cyber, Human Factors and Physical Security
 - Principals can also apply generally to risk assessments.

Security Matrix – Trends/Gaps and Recommended Focus Areas

Security Considerations	Cyber	Human	Physical	Trend approaching 2015
Identity Management (“AAA”)	↑	↑	OK	Ubiquitous Strong Authentication will be a requirement because of access to shared multiple apps environment. Also machine to machine authentication.
Crypto Key Management (certify users)	↑	↑	OK	More dependency on services/apps – more emphasis on certification of individual using “any device” from “anywhere”.
Account Management (user id/password mgmt)	↓	↔	OK	Human decisions/monitoring will continue to be critical. (On track). More automation and tools will be available.
Surveillance/Monitoring (identification/prevention)	↑	↔	OK	More need for physical surveillance. New tools will be available for Cyber monitoring. Human factor still required.
Malicious Attacks (intrusion, DOS, Physical security)	↑	↑	↔	Shared applications and inter-enterprise communications will open more doors for cyber based intrusion
Secure Transmission (encryption)	↑	↔	OK	All interactive communications will be encrypted. New “user friendly” techniques with stronger crypto
Back-up/Recovery (BCP’s)	↑	↔	↔	Dependency on shared multiple applications will increase the need for Business Continuity Plans and robust networks and IT infrastructure
Surveillance/Lawful Intercept	↑	↑	OK	Virtual “Anywhere, Any Device” environment adds to challenge

↑ Increased Focus ↓ Decreased Focus ↔ “Stay the course” Continuous improvement OK Existing policies meet requirements

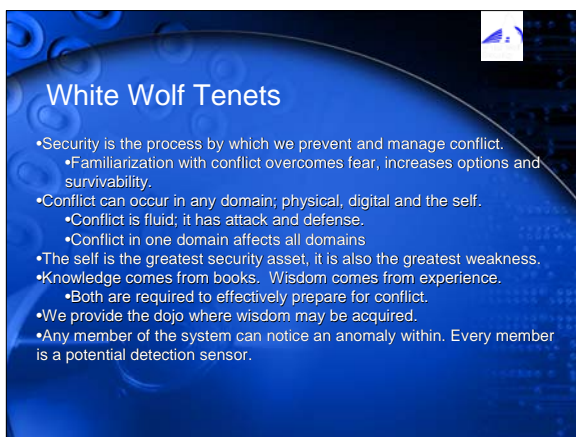
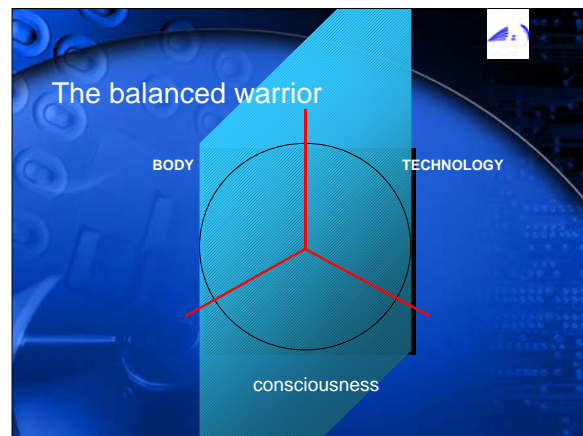
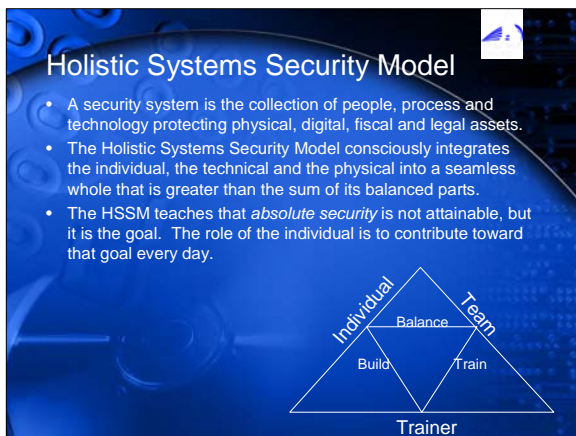
Summary – Potential Focus Areas

- Canadian Economic and Security Environment will drive the need for cost effective, collaborative communications environment with Global reach.
 - Converged, IP based communications infrastructure
 - Users seamlessly cross between multiple broadband mobile and wireline based access networks.
 - Protection of Business/Government Intellectual Property and collaborative communications tools for LEA’s/Security Services would dictate the need for higher security
- Physical, building and network infrastructure security is “well in hand”
- Devices will play an important security role
 - Potential focus areas – cost effective biometrics on “handheld devices”
- Vulnerabilities/Security Risks
 - IP based collaboration between Enterprises will open new doors for intrusion/attack
 - Centralized and shared directories, switching environments and applications represent the greatest security threat.
 - Cyber and Human Factor focus
 - Potential focus areas:
 - Ubiquitous strong authentication (M2M) and certification of individuals
 - Malicious attacks (Intrusion, DOS, Physical Security)
 - Need for stronger encryption due to introduction of Quantum computing
 - Business Continuity Planning and Robust Application Layer.
 - Weakest Link in shared application environment poses highest risk factor

Questions/Discussion

- Very open to discussions/opinions over next few days
- Contact Information – after conference;

Steven Featherston
 VoI Solutions Inc.
 613-837-7131 (office)
 613-859-1570 (cellular)
sfeatherston@voi-solutions.ca



2015

- We cannot predict the future.
- Current trends show increases in embedded technology and rapid convergence of cyber and physical domains.
 - The terrorists welcome this. We are afraid of it.
- Integrated operations are possible today with COTS solutions.
 - The availability of such programs will only increase.
- Training field personnel how to integrate cyberspace operations into physical operations can be accomplished in weeks, not months.
 - Good news/Bad news

Recommendations

- Integrate cyberspace into physical operations.
- For example:
 - Is technology the mission (controlling a communication network)
 - Is technology complementary to the mission?
 - Can our use of technology positively influence the mission?
- Pushing decision making down to the lowest level and self-synchronization
- The former professional Military Man's perspective
 - Teach warriors at the small unit level to seek out and exploit network and technological advantages. Truly turn every warrior into a sensor.
 - Network mapping (wired and wireless) should be as common a task as navigation and personal weapon maintenance.
 - This should apply to anyone who touches a keyboard

Tracking

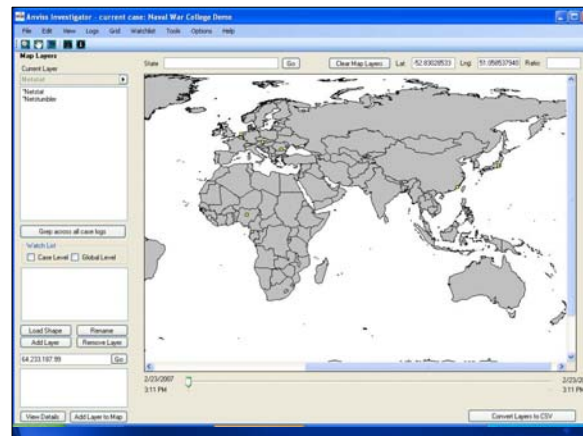
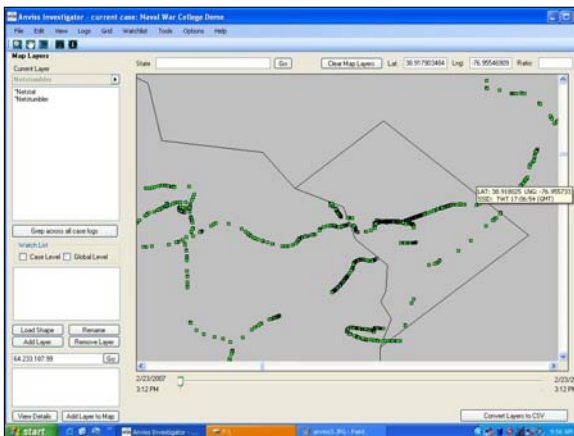
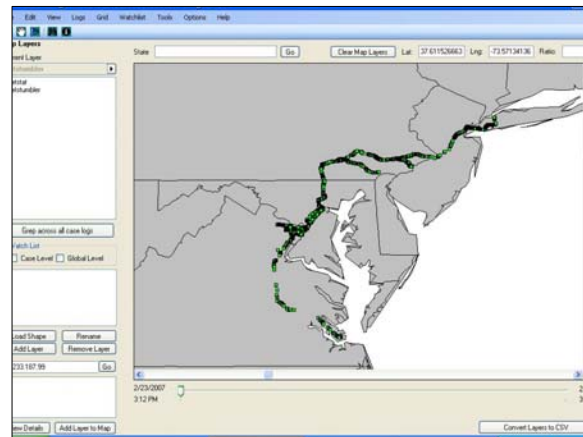
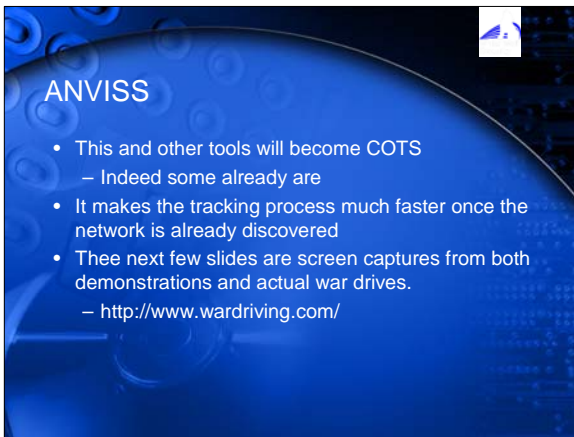
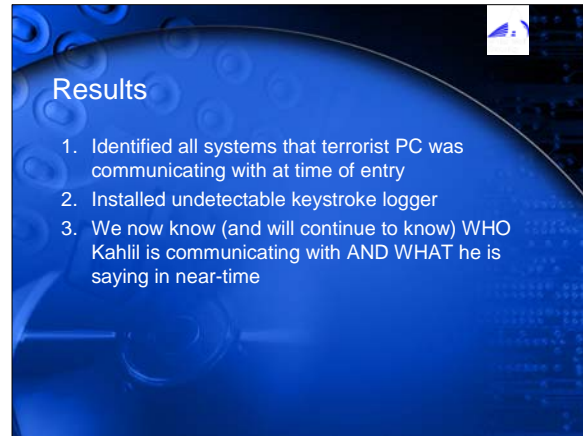
- Tracking via the Internet is time intensive as you are always looking for a moving target.
- It is trivial to obfuscate, randomize and anonymize traffic across the Internet.
 - Meaning – it is hard to track people based on chat rooms and web sites.
- Shift the focus:
 - Use HUMINT to find the terrorist networks
 - Use Cyber-INT to compromise the terrorist network from within
- Compromise the communication network and monitor known traffic and communications.
 - Follow this to new traffic and communications. I will introduce some tools for this a bit later.,

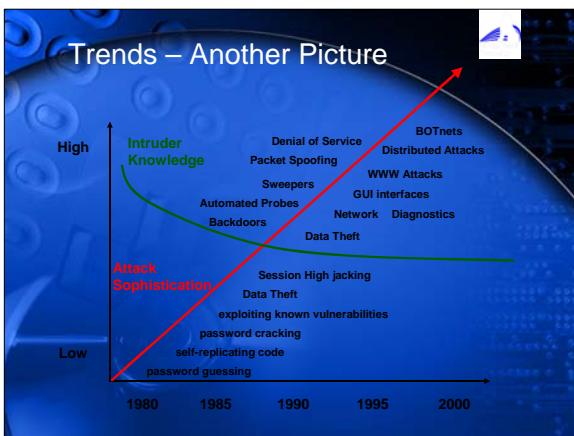
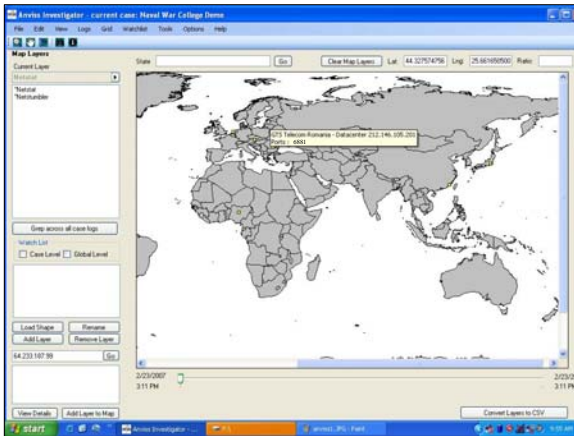
CONVERGENCE. CONVERGENCE. CONVERGENCE.

Using CYBER-HUMINT to Compromise a Terrorist Network from Within

How does this help now?

- Digital recon/ attack and defense gives greater depth to the battlefield.
 - It forces an enemy with somewhat limited resources to fight on another front.
- It allows us to retain the initiative by intercepting their global traffic at the tactical level and then using that link to disrupt their C2 globally.
- It gives us another intel and analyses weapon which will further lead to a greater understanding of the enemy's breadth and scope. This also gives us the critical link between the operational and the tactical level whose knowledge it allows its exploitation.
- This is real time off the shelf stuff and can impact the battlefield now.





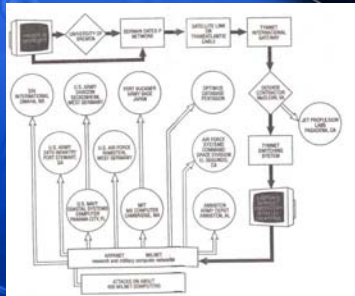
Hacker types

- The hacker threat refers to that non-structured threat entities that act alone
 - no sponsorship of a larger organization/country.
 - Here, I am referring to the 16 year old kid, hacking from his computer in Russia.
- The transnational threat refers to the gray area in-between hackers and nation-states.
 - This threat includes terrorist organizations, narco-traffickers, industrial espionage, etc..
- Lastly, the nation-state is the most dangerous of the three, since nation-states have a full arsenal of information warfare tools at their disposal.

The typical 'hackers'

- Since hackers usually act alone and do not have organizational sponsorship, their attacks will typically use well-known tools & techniques.
- They do not have an organizational objective
 - their attacks are carried out at the whim of the individual hacker.
- Regardless of whether it's being done for profit, fame, or control, a hacker's attacks will be far more frequent while the damage can range from "nothing" to the extreme (e.g. denial of service against Yahoo, etc.).

Island Hopping



From Clifford Stoll's: A Cuckoo's Egg

Transnational threats-terrorists and such

- The transnational threats, by comparison,
 - are usually group-oriented in nature
 - share a common cause.
- these threats typically appear when there is a cause to rally behind, they are seen much less frequently.
 - they rarely have organizational or state sponsoring
 - their tools & techniques closely mirror the individual hacker threat, yet they can be a little more sophisticated.
- The results of the transnational threat is typically
 - theft of data (industrial espionage),
 - manipulation of data for profit (narco-traffickers),
 - manipulation of data (web site hacks) to heighten world-wide awareness for a political/ethnic cause.

Nation on Nation Hacking

- The nation-state threat is least likely to occur (due to the political, legal, and military ramifications),
- Will be the most damaging when it does due to the large pool of resources available to nation-states to develop their capability.

The bad news

- You cannot un-invent bad technology
- Ubiquitous technology = ubiquitous threat
- You cannot de-tech the West
- Our adversaries are integrated
 - The same group will hack you just as easily as they will shoot you.
- Since the 1990's we have acknowledged that narco-nationalists, international terrorists, organized crime groups and racially motivated groups have worked and trained together.
 - They continue to integrate while the west continues to stovepipe.

More bad news

- Developed nation policy does not support a pro active approach to operations in cyberspace
 - It is a defense only environment more concerned with attack attribution than attack mitigation.
 - You can secure your systems or log off. There is not right to digital self defense in the US, Canada or the UK.

The threat space

- Blended (read convergence)
 - Physical
 - Infrastructure risks
 - Transportation
 - Medical
 - Telecom
 - Utilities
 - Financial
 - Global nature of economics make a hack induced crash of Wall Street, the LSE, or Hong Kong at least a regional issue
 - For ideologues financial districts are the symbolic grail of attacks.
 - Informational
 - Mass disinformation about the scope and nature of disasters or where to go for assistance.
 - Massive disinformation thru traditionally credible sources to an info junkie populace

Threats

- Mass
 - Distributed and below threshold attacks
 - High volume, low risk, collective high impact, single impact very low
- Precision
 - Single, targeted attacks against critical infrastructure
 - Low volume, high risk, single impact very high
- Hackers do not need a reason to hack you. They may not be motivated by anything more than the challenge or the cash or the boredom or patriotism.

Threat Actors

- Economic competitors
 - Foreign and domestic
 - If you thought industrial espionage was a problem in the 1980's you haven't seen anything yet.
- Organized crime
- State sponsored
- Clowns who just want to hack and found your system to be an appropriate challenge.

Who dunnit doesn't matter

- The need to attribute precise source of attack is putting the cart before the horse.
- If you are under electronic attack:
 - Stop the attack through proportional and necessary means (digital self defense)
 - Mitigate damage
 - THEN find out who really did it.
- Current response models in developed nations waste time trying to ascribe proper responsibility.
 - Use your resources to stop and reverse. Then seek justice.

Some Case Studies

Case study 1

- F-22 Raptor 2006
- This was absolutely an accident
 - It was also a wake up call
- Imagine if an adversary had the ability to cause said 'accidents' at will or on demand
 - Imagine this not only for military operations, but what about humanitarian or SOSO.

Case Study 2

- Blue Security
 - <http://www.securityfocus.com/news/11392>
- Key things
 - "We cannot take the responsibility for an ever-escalating cyberwar through our continued operations,"
- Controlling escalation in Cyberspace
 - Without a physical 'hammer' no one will ever care.

Swedish bank hit by 'biggest ever' online heist

January 19th 2007
<http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm>

Overview

- Nordea (Swedish bank) had its' customers targeted with a custom trojan sent via email.
- The email encouraged clients to download a tool to fight spam. The tool was actually a trojan that logged keystrokes when infected users attempted to log into the Nordea home page.

More overview

- The tool redirected users to a fake login page that captured credentials.
- The stolen credentials were then used to transfer money out of the customers' accounts.
- The attackers are believed to be Russian OC who kept the bank transfers relatively small in order to make them look like legitimate transfers.

And I quote:

- "In some cases we saw the transactions were false, and in some cases we didn't", said Ehlin. [Nordea spokesman for Sweden] "We can't look at every transfer, and it looked like our customers had made the transfer. Most of the cases were small amounts that we thought were ordinary. We lost approximately seven to eight million krona."

METAVERSES

Metaverses

- Creates another area for traditional terrorist activity
 - Dead drops for both information and programs
- Creates jurisdictional nightmares
- Are not currently traceable
- Create opportunities for the good guys also
- Also create an economy within an economy

The Virtual Center in Second Life



RECOMMENDATIONS

Tools/skills we need:

- Tools that reflect the physicality of cyberspace like Anviss
- Cross trained individuals capable of fighting/defending in both the cyber and physical combat spheres.
- Reliable off the shelf defensive/offensive tools
- Good network design and hourly vigilance.
- Sys-admins need to be warrior like in their approach to network defense.
 - The Zen of network security
 - Anomalies happen. Understand why they happened. Do not simply accept hiccups.
- Stay on top of trends
- And a policy that supports their effectual and timely use.

Now for Something Completely different

- We can't un-invent the threat but we don't have to accept victimization either.
- Decentralize the defense process and enlighten the masses
- Good solid network design
- Stay abreast of the trends
- Understand that you are always vulnerable
- Develop redundancy in critical infrastructure pieces
- Coordinated kinetic-cyber response.
- Train at White Wolf Security

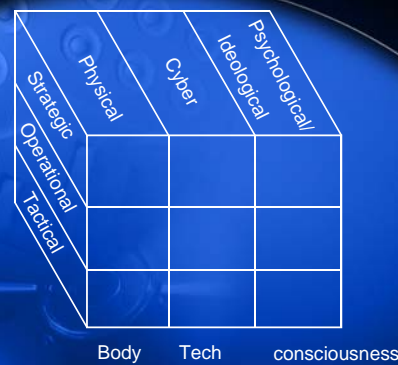
Recommendations

- Integrate cyberspace into physical operations.
- For example:
 - Is technology the mission (controlling a communication network)
 - Is technology complementary to the mission?
 - Can our use of technology positively influence the mission?
- NCW is partially about pushing decision making down to the lowest level and self-synchronization
- Teach warriors at the small unit level to seek out and exploit network and technological advantages. Truly turn every warrior into a sensor.
 - Network mapping (wired and wireless) should be as common a task as navigation and personal weapon maintenance.

What questions can I answer for you?

Supporting Material

Military Convergence



Current ISR Doctrine & TTP Overview

- Friendly technology based stand alone ISR
 - Real time available UAV's, satellite imagery, IR passive and active, etc
 - We are fixated on the machinery
- Technology incidental to operations
 - Find PC by chance during C&S or similar raid
 - Secure room
 - Take PC
 - Conclude op
 - Turn box over to some intelligence guy and you never see the info again

Extrapolating current trends to the future

- Convergence
 - The cyber and kinetic worlds are one and the same.
 - If can push a button and shut down infrastructure the two worlds are one and the same
- Mobile
 - Attackers can move two ways-thru the internet and physically. Defenders should be able to do so as well
 - Redundancy in critical infrastructure is a key
 - Keep it on the down low

SO WHAT?

- Currently intel collection and analysis are separated from physical and cyber domains.
 - ISR and ops are disconnected by space/process
 - Intel collection is stove-piped from operations
- No single group in the field is doing both
 - Therefore, when an operator comes across technology in the course and scope of an operation, their job is to seize and pass back for analysis.
- The separation of physical and cyber operational domains results in several negative 2nd and 3rd order effects:
 1. Increases the time from seizure of intel to being able to act on it.
 2. Increases our decision cycle
 3. Greatly reduces mission flexibility
 4. Does not address a connectedness between physical and cyber operations that not only exists but that is successfully being exploited by our enemies

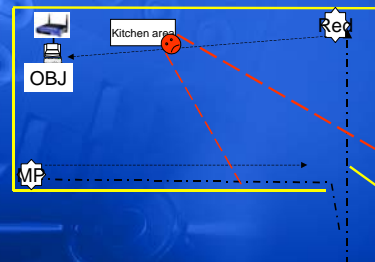
Cont

- Red & Mr. Pink will infil with the contact. He will transport us in the back of a pick up marked with an Ace of Spades in the windshield. He will drop us at the de truck point at 2145. He will NOT BE IN THE AO DURING THE OP.
- Tim will acquire the visual camera signal as we move in range.
 - Red will call for the DDoS when room is verified clear. On confirmation of DDoS we will complete infil on foot.
 - Point of no return is the doorway.
 - Abort criteria is
 - more than 2 people in the room on camera
 - Abort from higher or me
 - Compromised on that street within 1 block of the door.
 - Too much time on the obj / irresolvable install problems
 - The camera alarm signal is not jammed

Execution cont

- Task Org for this looks like this
- The team will be split into three entities.
 - Inside team – Mr. Pink and Red (pistols only/civilian clothes)
 - Outside team – Smitty, Booth, TR, Chief, Gonzo, GT. You will be part of the patrols in the AO. You will be stationed along Al Kahlil's infil and exfil routes to provide us with early warning.
 - Roof team – Big Tony & Longbow, you will have the radio link to higher and set up one sniper overwatch position. Angry and Doc you two will set up sniper spotter positions on the higher rooftops in the neighborhood at H-1.5.
 - Remote team – D'Mo on ship to execute DDoS against target IP to secure electronic surveillance. (Deny use to target, enable use by Inside Team)
- The Critical tasks are to gain uncompromised entry to the house, compromise the box and uplink to the command center on ship. Once that is done D'Mo can gain his network map, read and control his traffic.

Actions on the Objective

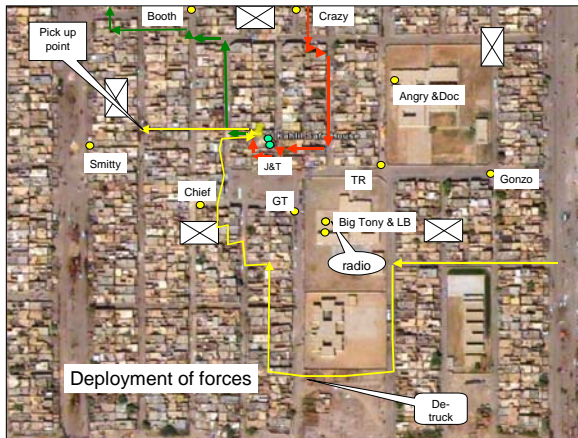


Exe cont

- We go with a two man entry team because three guys draws attention. Two is no big deal. Inside team will go in plain clothes. And use only pistols (conceal-ability). Outside team is in conventional uniform-make sure that you match up for gear-no cool guy stuff.
- Outside team you have the inside team's outer security and comms higher. You will have the satcom. Pass and monitor traffic.
- The separate teams will link up with their prospective Marine units NLT 1500 hours. Make sure your gear looks like theirs. You will infil into the AO with them. All personnel will have their ICOMS and MBTRs on the team push. Call set when in place.
- Roof teams will go immediately to their rooftops. Big Tony, get comms with higher immediately when you are secure and let me know.

cont

- Red installs root kit and ANVISS. We pass traffic to D'Mo.
 - On confirmation that D'Mo has the box we exfil.
- Go due west to Smitty's position. We will call D'Mo to end DDOS.
- Smitty and 1st Squad 2nd Plt pick us up as violators, hood us zip cuff and haul us back here.
 - If less than 3 in the room. We will take them down.
 - On exfil we will call for pick up and Smitty will get the lot of us.
- Roof teams break down as soon as inside team is rolled up.
 - Link up with the squads you rolled in with
 - Break down and bag the long guns.
- We will be carted off immediately. Patrols will remain for an additional ½ hour from departure
 - Big T call 'package tight' to higher when inside team rolls out of AO.
- Support for this op is A Co 2nd plt
 - Inside team is going with the source
 - Everyone infils / exfils with their Marine squads
- Comms is by SOP everyone keep their respective patrols' push locked on channel 5.
- Red and Pink have D'Mo on channel 6





Smart Technologies

Originally presented at
World Future Society
July 29, 2006
EDS Fellows Canadian Tour
Sept 11-12, 2006
PACT
Sept 19-20, 2006

Global Security Scan for
Canadian Science Capabilities
CRC Shirley's Bay
Ottawa, On Canada
March 21-23, 2007
Presented by Walter Derzko

Outline-The Smart Economy 7 Overview Topics

- What is a smart technology? Definition
- Categories
- Examples
- Impacts and Consequences of Smart Technologies
- Roadmaps
- 12 Smart Technology Trends
- 2020 Capabilities > Magic Blocks



Nanotech? Biotech ?Info ?

- Nanotech? Biotech ?Info ?
- What's the common denominator?
- Things become smarter; more intelligent
....both for the good guys & bad guys
- Changing landscape? Ground rules?



Definition

- What Makes a System /Object Smart?
- Generally speaking, if a machine/artifact does something that we think an intelligent person can do, we consider the machine to be smart.



Misnomers

- Smart Car ? Intelligent or Stylish?



- Various adjectives:
smart, intelligent, active,
dynamic, wise


The VW "Golf Gti 53 plus 1" has
radar and laser sensors to "read"
the road and send the details back
to its computer brain.

Drivers Wanted ...to....Drivers Optional



Outline-The Smart Economy 7 Overview Topics


- What is a smart technology? Definition
- Categories
- Examples
- Impacts and Consequences of Smart Technologies
- Roadmaps
- 12 Smart Technology Trends
- 2020 Capabilities > Magic Blocks



How do I know if I have a smart technology?


You can't paint all products with the same "smart" brush.

•Recognizing that some products or technologies are smarter than others, we have developed an intelligence scale to distinguish between levels of "smartness" or intelligence.



Intelligence Level (1)	Adapting:	Modifying Behavior to Fit the Environment	
Intelligence Level (2)	Sensing:	Bringing Awareness to Everyday Things	
Intelligence Level (3)	Inferring:	Drawing Conclusions from Rules and Observations	
Intelligence Level (4)	Learning:	Using Experience to Improve Performance	
Intelligence Level (5)	Anticipating:	Thinking and Reasoning about What to Do Next	
Intelligence Level (6)	Self-creating,	Able to reproduce itself	
Intelligence Level (6)	Self-organizing	Ability for components to self-organize	
Intelligence Level (6)	Self-sustaining (A)	Ability to replicate components	
Intelligence Level (6)	Self-sustaining (B)	Ability to process information	
Intelligence Level (6)	Self-sustaining (C)	Ability to steadily consume energy from the environment	


© 2005-2006 Walter Dertzko



Intelligence Level (1)

Adapting: Modifying Behaviour to Fit the Environment


- Adaptive networks, GPS, directory services, collaborative filtering, humanized interfaces,
- Basic adapting objects i.e smart clothes



Intelligence Level (2)

Sensing: Bringing Awareness to Everyday Things

- Sensors, embedded systems (smart badges, smart bricks, smart bridges, smart levees,) smart environments, smart materials (smart cement, packaging), smart cameras, smart doors



Intelligence Level (3)

Inferring: Drawing Conclusions from Rules & Observations


- Expert systems, knowledge bases, inference engines, fuzzy logic, basic AI
- Darpa Grand Challenge --Driverless Car Race-front end logistics



Intelligence Level (4)

Learning: Using Experience to Improve Performance


- Subfields of Advanced AI; Case Based Reasoning (CBR), neural nets, genetic programming,
- intelligent agents , AUV's, Exoskeletons

 Intelligence Level (5)
Anticipating: Thinking & Reasoning about What to Do Next

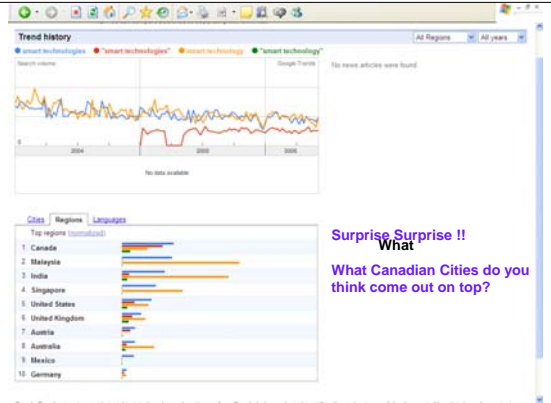
- goal-directed systems, robots, artificial life software,
- Smart mind-controlled wheelchair

 Intelligence Level (6) Self-Organizing: Self-generating at the cellular or nano level

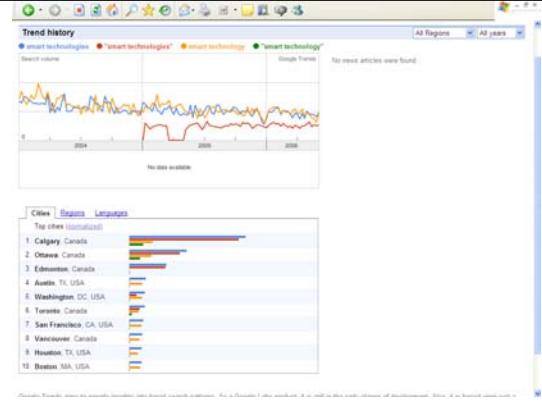
- Self-organizing systems, complex awareness, cognition, self-reproduction and self-healing, if injured

 The Smart Economy

- Who is interested in Smart Technology?
- Use Google Trends
- What countries come out on top?....any Guesses ?

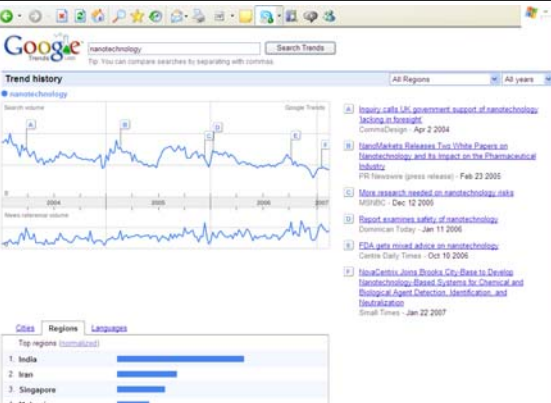


Surprise Surprise !!
 What
 What Canadian Cities do you think come out on top?



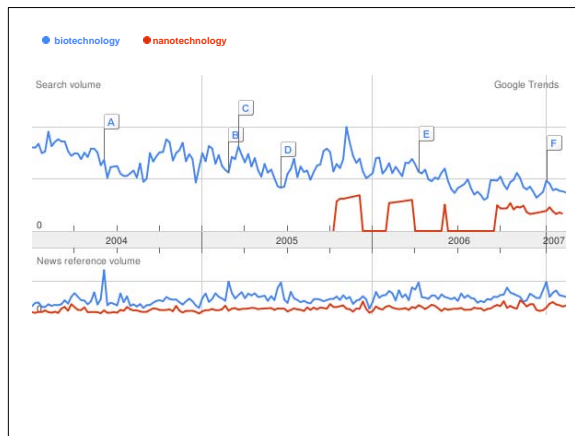
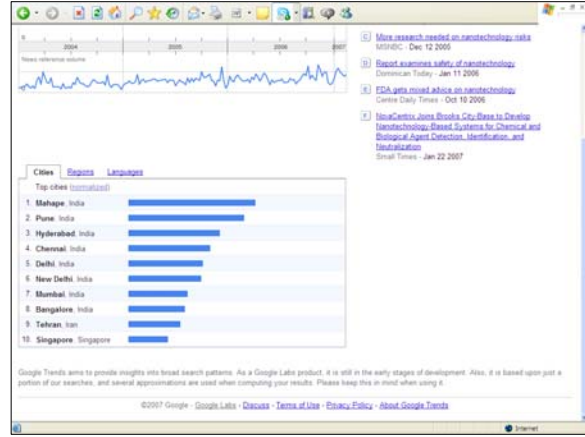
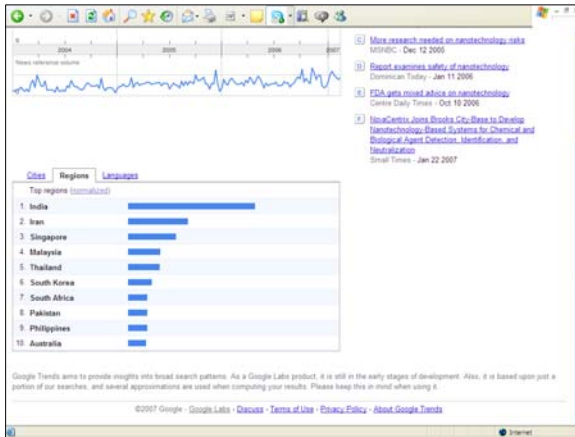
Top cities (unranked)

Rank	City
1	Calgary, Canada
2	Ottawa, Canada
3	Edmonton, Canada
4	Austin, TX, USA
5	Washington, DC, USA
6	Toronto, Canada
7	San Francisco, CA, USA
8	Winnipeg, Canada
9	Houston, TX, USA
10	Boston, MA, USA



Top regions (unranked)

Rank	Region
1	India
2	Iran
3	Singapore
4	Malaysia
5	Thailand



Outline-The Smart Economy 7 Overview Topics

- What is a smart technology? Definition
- Categories
- Examples
- Impacts and Consequences of Smart Technologies
- Roadmaps
- 12 Smart Technology Trends
- 2020 Capabilities > Magic Blocks

Smart Technology Impacts?

1) What gets Enhanced?

2) What gets Retrieved? Brought Back

3) What gets Obsolesced? Left Behind?

4) At the extreme, What gets Flipped or Reversed?

Tetrad Automobile & Infrastructure

1) What gets Enhanced?

2) What gets Retrieved? Brought Back

3) What gets Obsolesced? Left Behind?

4) At the extreme, What gets Flipped or Reversed?

Infrastructure in Peril

The following is a brief laundry list of the current state of US infrastructure.
The outlook isn't pretty:

- 33% of major roads are considered substandard
- \$5.8 billion cost to drivers
- 13,800 highway fatalities per year
- 29% bridges considered structurally deficient
- \$10.6 billion cost to fix bridges
- 50,000 flight delays at nation's airports
- 75% of school buildings deemed inadequate
- 54,000 drinking water systems deemed inadequate
- 16,000 waste water systems near collapse
- 2,100 dams classified unsafe
- 44% inland waterway systems obsolete
- 30% annual shortfall in electric capacity



The greater the infrastructural outlay of a civilization, the greater the resources required to maintain it. As energy concerns mount, this maintenance becomes that much more expensive. In addition, resources dedicated to maintenance alone begin to outweigh those dedicated to creative research and development, and the available energy per capita goes down

N.B. when Rome began to fall, the maintenance demands on its expansive infrastructure had reached a critical limit with fewer energy returns per capita...

Source: "Renewing America's Infrastructure: A Citizen's Guide," American Society of Civil Engineers, 2001, pp. 3, 6-7

Smart Technology Impacts?

- Pervasive, Ubiquitous
- Disruptive (think computers & secretaries)

Smart Technology Impacts?

- Pervasive, Ubiquitous
- Disruptive
- As great as the emergence of writing, language & the PC
- Look for obvious & hidden 2 & 3 effects
- Creeping up silently on society

Smart Technology Impacts?

- Pervasive, Ubiquitous, Disruptive
- As great as the emergence of writing, language & the PC
- Look for obvious & hidden 2 & 3 effects
- Creeping up silently on society
- What controls do we have over adoption?
- Erroneous assumption that everything will be positive

Smart Technology Impacts? Duel Use; Double Edged Sword

Intelligent Agents;

(+) **Positive Aspects** : crawl around the internet ie. eBay Comparison shopping

(-) **Negative Aspects** : IEEE International Conference on Intelligence and Security Informatics, May 2006

Smart Technology Impacts?

- DOS attacks> Smarter Malware? > Holy Grail ? >>Smart Theft Engines?
- Abstract:
- "A network is not secure unless it can ensure the three basic security concepts; **confidentiality, integrity and availability**... [...] Here we show a highly personalized attack by the use of **specialized agents** whose purpose is to search and transmit specific information from a private network without authorized access."
- This information may be in the form of a competitor's marketing strategy, customers' personal details, true financial status of an organization or any other information. We discuss that such an agent and its activity is different from common malware, describe its characteristics and design and show that such a scenario is a **real possibility**. We also discuss the related issues and the alarming effects posed by such an agent. It is possible that the agent we are discussing may already be in existence but are unreported**.
- [**this already exists from a reliable source]
- How can you tell that your system has been breached?
- Bank robbers > Pearl Harbor> DOS> Theft Engines?

Smart Technology Impacts?

- Pervasive, Ubiquitous Disruptive
- As great as the emergence of writing, language & the PC
- Look for obvious & hidden 2 & 3 effects
- Creeping up silently on society
- What controls do we have over adoption?
- Erroneous assumption that everything will be positive
- Google "smart technology" July 27, 2006 > 300 Million hits
- No standards, no regulations yet; fragmented market

Smart Technology Impacts?

- Pervasive, Ubiquitous Disruptive
- As great as the emergence of writing, language & the PC
- Look for obvious & hidden 2 & 3 effects
- Creeping up silently on society
- What controls do we have over adoption?
- Erroneous assumption that everything will be positive
- Google "smart technology" July 27, 2006 > 300 Million hits
- No standards, regulations yet
- Not in the public mindset yet Lack of public discourse,
- Very few Media have grasped the significance yet

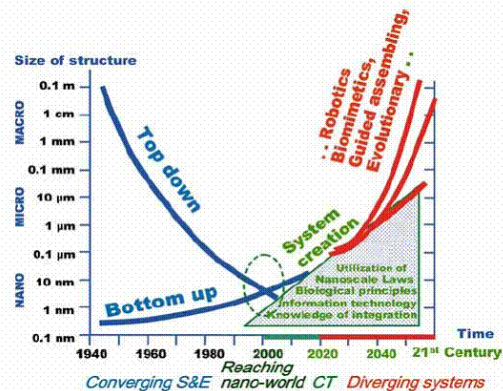
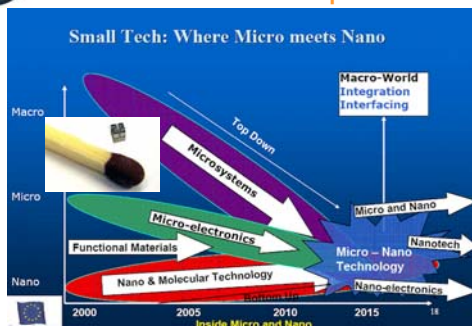
Outline-The Smart Economy 6 Overview Topics

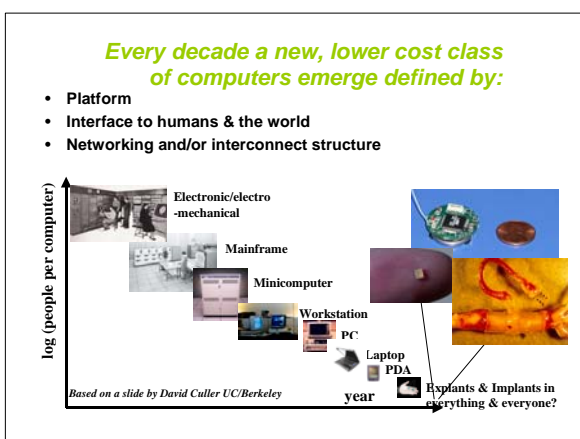
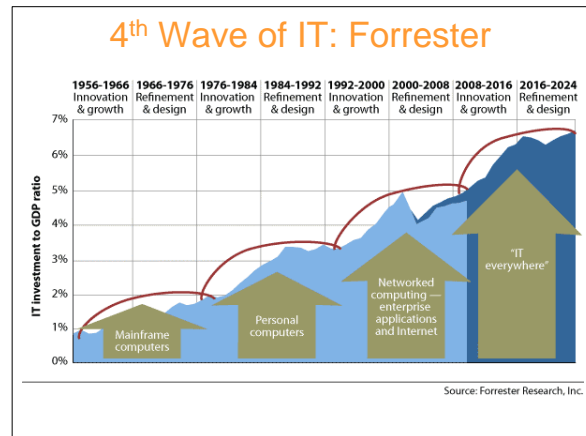
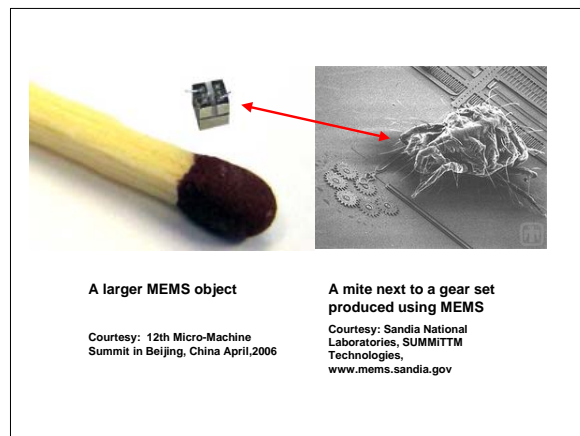
- What is a smart technology? Definition
- Categories
- Examples
- Impacts and Consequences of Smart Technologies
- Roadmaps & Drivers & Barriers
- 12 Smart Technology Trends
- 2020 Capabilities > Magic Blocks

How will the Smart Economy evolve? Thought Leaders

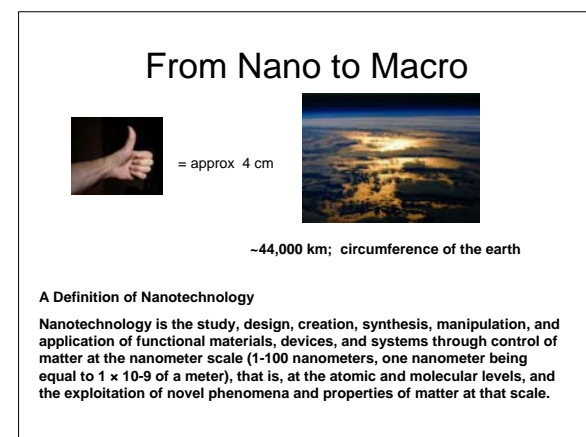
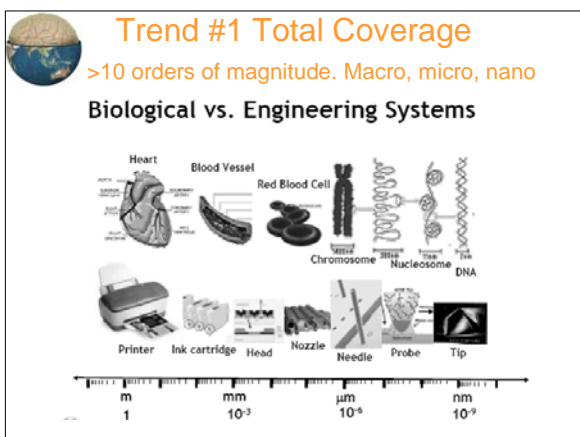


EC Roadmap





- ### Outline-The Smart Economy
- #### 6 Overview Topics
- What is a smart technology? Definition
 - Categories
 - Examples
 - Impacts and Consequences of Smart Technologies
 - Roadmaps & Drivers & Barriers
 - 12 Smart Technology Trends
 - 2020 Capabilities > Magic Blocks



Trend #2 Man-made objects mimic Bio

- MIT engineers have found a way for structures and materials - to move [like birds' wings]... essentially morphing from one shape into another.
- A UC Berkeley project aims to replicate gecko hair as an adhesive
- Architects have designed smart buildings that breath (control CO2) and blink (regulate sunlight)
- Researches mimic spider and fish hairs that detect air/water currents & movement

Gecko adhesive system

Macro Meso Micro Nanostructures

Trend #3 External Power → Self-Generated Power

Macro

Electro-Kinetic Road ramp

Regenerating Brakes

Add 1 photon of sunlight; get 2 electrons' worth of electricity

Micro

Trend #3 External Power → Self-Generated Power

Glow-in-the-dark Nano-particles

Piezoelectric effect

Gold Nanoparticles hot

Trend #4 Single Function → Integrated Systems (LAN → BAN)

Development of **Capsule Endoscopy** and **Micro Biomedical Diagnostic System** Using Intelligent Microsystem and Integration Technologies

In-Vivo System
Micro Capsule

In-Vitro System
Diagnostic LabChip
POC System

BioMedical System

Trend #4 Single Function → Integrated Systems

Intelligent Microsystems

Micro Biomedical Diagnostic System = Walking Hospital

The system enables doctors to screen and check the conditions of patients, and treat diseases ubiquitously.

Preparation : Cell lysis

Immobilization & Detection

Sampling

Microfluidics

Nano and Micro Technology in Korea


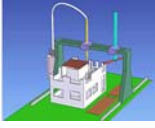

World Micromachine Summit 2005

Trend #4 Single Function → Integrated Systems

Decorative Tattoos

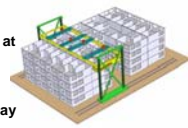
Functional Programmable (Medical) Tattoos


Trend #5 Smart Objects → Smart Processes

**2D Printer → 3D Rapid Prototyping
Now....3D Contour Crafting**

**S. Africa looking at
"printing" 10M
housing unit
over next
10 years= 2747/day**





Trend #6 Expect Big Surprises

"It might be assumed that the flying machine which will really fly might be evolved by the combined and continuous efforts of mathematicians and Mechanicians in from one million to ten millions years—provided, of course, we can meanwhile eliminate such little drawbacks and embarrassments as the Existing relation between weight and strength in inorganic materials."

The New York Times (October 9, 1903)

Trend #6 Expect Big Surprises

"It might be assumed that the flying machine which will really fly might be evolved by the combined and continuous efforts of mathematicians and Mechanicians in from one million to ten millions years—provided, of course, we can meanwhile eliminate such little drawbacks and embarrassments as the existing relation between weight and strength in inorganic materials."

The New York Times (October 9, 1903)

Footnote:
On December 17, 1903, (a little more than two months later), at Kitty Hawk, North Carolina, the Wright Flyer became the first powered, heavier-than air machine to achieve controlled, sustained flight with a pilot aboard



Trend #6 Expect Big Surprises

Who will solve the Climate Change/Global Warming & Fuel Crisis?



Lord John Brown, BP



Richard Branson, Virgin Fuels

****Distributed System?***

Boron + H₂O? →

CO₂? →

You and Me? Your local Farmer?

Veg Oil + Alcohol = Instant Bio diesel




****LD Wireless Power?***

****Synthetic Porphyrin?***



Trend #6 Expect Big Surprises

Detroit's Biggest Nightmare?
Not Honda or Toyota



The car of the future could likely come in a box and will be delivered via FedEx.

Need a new part? Just go online and order it.




Think FedEx, not car dealerships.
Think smart engine modules that pop in and out, not auto mechanics.
Think Wal-Mart, not Midis Muffler

Source: Jim Carroll's Blog

Trend #7 Big Shift; Silicon to Non-Silicon MEMS

	In Development	Established Products
Silicon	Micro cooling Devices MEMS memories efuses	Read-Write Heads MEMS display Pressure sensors Flow sensors Accelerometers Gyroscopes Micro machined Probes Fingerprint sensors IR sensors, Microphones
	Micro Power Sources	Ink Jet heads: Si, metal, polyimide
Non Silicon	Micro pumps Thin film plastic chips (flex electronics)	Micro-fluidic chips: glass polymer Spray Nozzles for drug delivery: polymer Micro-motors: piezo-electric
	Micro Reactor: metal Liquid Lenses: MEMS display	

**Trend #8 Convergence
Bio+Inorganics**






**Trend #9 Hobbyists give Smart
Technology a push**

Circa 1970

PC Industry born with the help of garage hobbyists

Would you invest in this company?



**Trend #9 Hobbyists give Smart
Technology a push**

Circa 1970

PC Industry born with the help of Garage hobbyists

Would you invest in this company?




**Trend #9 Hobbyists give Smart
Technology a push**

Circa Aug 2006
LEGO publicly launched Mindstorms NXT


"smart bricks"

Cartoonist's portrayal




Think "Windows OS" for Robots

June 2006
Microsoft Robotics Studio



**Trend #9 Hobbyists give Smart
Technology a push**

Korea to Unveil Programmable Robot
– a 30 cm tall, 2 legged walker D2V-ZN in October 2006





- D2E Robotics
- S. Korean venture start-up
- Programs can be adjusted by users on personal computers
- Smartest robot on the market
- Fully programmable robot
- 700,000 won (\$732)
- down to 300,000 won when produced en masse

**Trend #9 Hobbyists give Smart
Technology a push**

**Robocup
Nanogram League (Proposed)**

- "The game of soccer was the original motivation for RoboCup. Besides being a popular worldwide sport, therefore an appropriate medium to attract people to an event, it contains a significant set of challenges for researchers"
- Leagues
 - Humanoid
 - Middle Size
 - Small Size
 - Four-Legged
 - Rescue Robot

<http://www.robocup.org>



Trend #9 Hobbyists give Smart Technology a push

**Robocup
Nanogram League (Proposed)**

- A new Robocup league for Microrobots (proposed)
- Demo will be at the next Robocup in Bremen, Germany 14-20 June 2006
- If approved, the first competition will be at the next Robocup June 2007



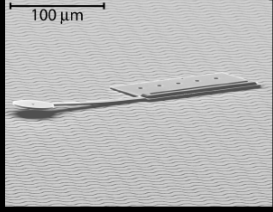
Committee: Craig McGary, Adam Jacoff, Michael Gertel, Timothy Arai, Satoshi Tadokoro

<http://www.robocup.org>



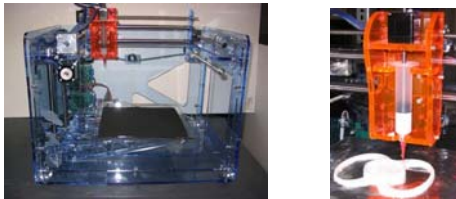
Trend #9 Hobbyists give Smart Technology a push

**Robocup
Nanogram League (Proposed)**



Journal of Microelectromechanical Systems, vol. 18, No. 1 (2009), pp. 1-15

Trend #9 Hobbyists give Smart Technology a push



Will cheap self-assembly devices capable of fabricating 3D objects kick start a revolution in mass-market 3D printing at home? – sometimes called "rapid prototyping" or home fabrication or fabbing?



Trend #10 Domestic Robots usher in Smart Technology Age



Mindstorms NXT



Akazawa's PLEN humanoid robot in Japan comes with roller blades



Robots at FIFA World Cup



Robocup



Trend #11 Designing Robust Viable Systems

"It is easy to turn an aquarium into fish soup, but not so easy to turn fish soup back into an aquarium."

- - Lech Walesa on reverting to a market economy.



Trend 12; Just because it's smarter, is it better?

Is "Smarter" always better?

Lifecare, Norway is developing an implantable glucose sensor

- Diabetes I and II are widespread and increasing in the population all over the world.
- Diabetes II over-represented in obese people: A lifestyle-related illness.
- Potential concept using osmotic pressure over a semi permeable membrane as a measure for the blood glucose concentration.
- Implanted in the wrist.
- Induction powered.
- External readout unit.
- Production start some years into the future.





Trend 12; Just because it's smarter, is it better?

- Constant glucose tracking may not improve outcomes
- Counter intuitive?
- Continuous monitoring-guided insulin adjustment appears to be no more effective than intermittent fingerstick monitoring in achieving control of blood sugar, or blood "glucose," in certain children with type 1 diabetes, Australian researchers report in the journal Diabetes Care.
- To determine whether a continuous system might achieve better results, the researchers studied 36 children. All of the subjects had slightly elevated glucose levels and were on intensive diabetes treatment with continuous insulin infusion by implant or insulin injections. The researchers conclude that although continuous monitoring might help certain groups of patients, it does not appear to offer any advantages in reasonably well-controlled outpatients.
- Source: Diabetes Care, July 2006.

Dilemma ?

- We are trying to plan for:
 - Technologies that have not been invented
 - Jobs that don't exist yet
 - Problems that we can't anticipate yet
 - Applications that we have yet to imagine
 - Risks that we can't quantify yet
 - Viable systems and Systems type thinking, that most people are not use to doing

We are now in March 22, 2020

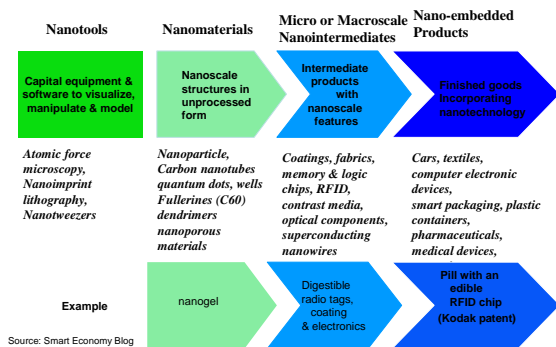


New Capabilities?



New Technologies?

Traditional Nanotech Value Chain





Source: Smart Economy Blog

Thank You for your attention & enjoy the rest of the workshop.

Please leave me your business card if you want a copy of the more extensive 1 hour presentation

Q & A





Working Together

Global Security Scan for Canadian Science Capability

March 21-23, 2007

Robert Crawhall, PhD, P.Eng.
President & CEO,
National Capital Institute of Telecommunications
crawhall@ncit.ca
(613) 998-5237

Working Together
Global Security Scan for Canadian Science Capability

NCIT Mandate

"To perform multi-disciplinary, multi-party, collaborative research involving the private sector, academia and government labs..."

.....its fun, but its tougher than you might think



Global Security Scan for Canadian Science Capability





About the NCIT

- Managed \$80M of collaborative research since 2000
- Telecom & eCommerce
 - Identity theft
 - Network and data vulnerabilities
 - Sensors, wireless
 - Healthcare,
- Research in Engineering, Science, Business, Law, Psychology, etc.

Working Together
Global Security Scan for Canadian Science Capability

The multi-disciplinary dynamic





Working Together
Global Security Scan for Canadian Science Capability



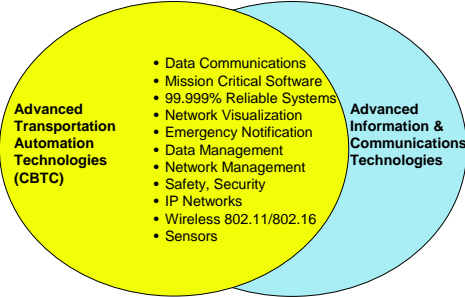

Shared Experience



Working Together
Global Security Scan for Canadian Science Capability

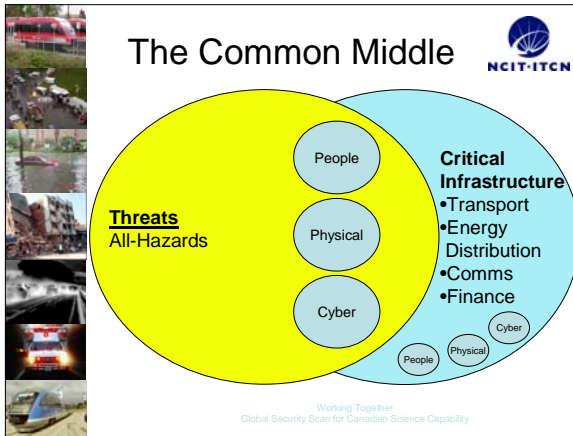



Cyber & Transport



- Data Communications
- Mission Critical Software
- 99.999% Reliable Systems
- Network Visualization
- Emergency Notification
- Data Management
- Network Management
- Safety, Security
- IP Networks
- Wireless 802.11/802.16
- Sensors

Working Together
Global Security Scan for Canadian Science Capability



Racing towards 2015

- Integration of communications-based urban transportation systems – train, car, bus, roads
- Safety and security of “open” communications systems
- Redundancy and interoperability of on-board communications systems satellite, cellular, BB wireless

In-Car Coverage WAN Challenges Multiple Onboard Applications

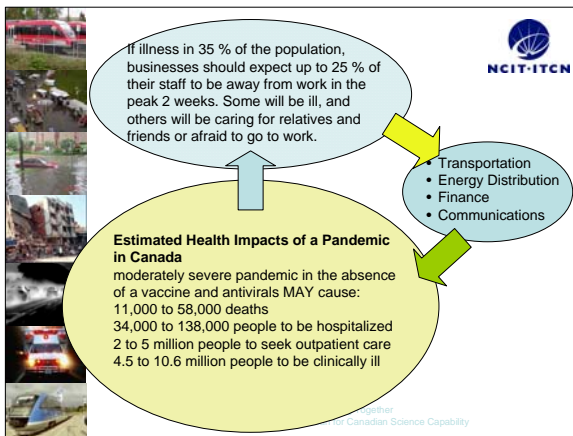
Working Together
Global Security Scan for Canadian Science Capability



Supporting Standards Development

- CIP applications are governed by strict standards. COTS Communications Systems do not necessarily comply:
- Train specific standards:
 - EN 50128 - *Software for railway control and protection systems: methods to provide software which meets the demands for safety integrity.*
 - EN 50121 Electromagnetic Compatibility – Railway Applications
 - EN 50126 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
 - IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.
 - prEN 50129 * *Safety related electronic systems for signalling*
 - IEEE 1474.1 CBTC Performance and Functional Requirements;
 - IEEE 1474.2 User Interface Requirements for CBTC

Working Together
Global Security Scan for Canadian Science Capability



Situational Awareness

- Embrace the diversity
- Challenge the conventional wisdom
- Look for specific leverage points that lead to common solutions

Working Together
Global Security Scan for Canadian Science Capability



Prepare for Something



Working Together
Global Security Scan for Canadian Science Capability



Vision

The Centre for the Protection of National Infrastructure, CPNI, will be the recognised government authority in the UK for protective security advice to the National Infrastructure.

It will:

- ✓ Minimise the risk to the National Infrastructure from attacks through physical, electronic or personnel means;
- ✓ Deliver authoritative, holistic protective security advice;
- ✓ Reduce the vulnerability of the National Infrastructure to terrorist and other threats.

CPNI
Centre for the Protection of National Infrastructure

What is CPNI?

A single Protective Security Business delivering physical, personnel & electronic security advice;

- ✓ 74% of NSAC users wanted access to NISCC advice on information security
- ✓ 76% of NISCC users wanted access to NSAC advice on personnel and physical security

2 identities merged



NISCC
NATIONAL SECURITY ADVICE CENTRE

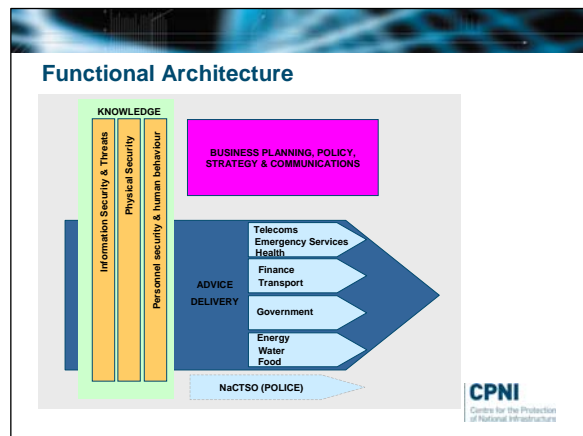
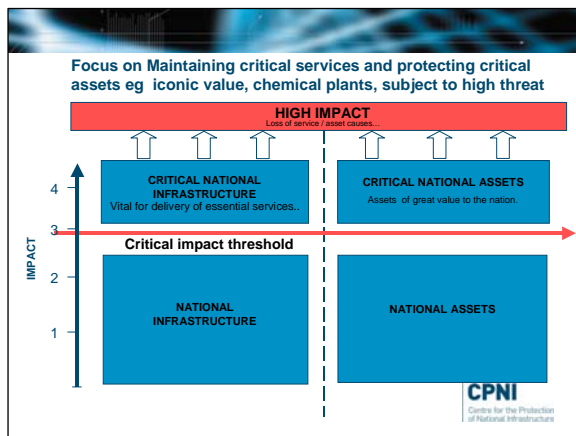
A new Brand recognisable by users as the UK Government authority on protective security advice for the national infrastructure.

CPNI
Centre for the Protection of National Infrastructure

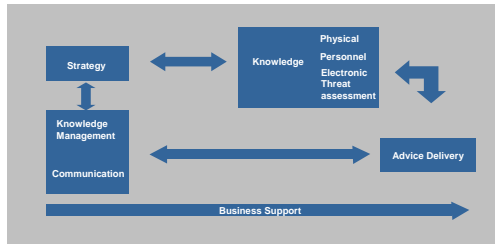
What sort of Business will CPNI be?

- ✓ Interdepartmental will include staff from other parts of Government, like CESG, and private sector.
- ✓ Accountable to the Director General of the Security Service
- ✓ Steering Group comprising others in Government and Private Sector
- ✓ Operates under the Security Service Act
- ✓ Focus on Critical National Infrastructure
- ✓ Product Leadership organisation

CPNI
Centre for the Protection of National Infrastructure



Integrated Process



Strategy and Policy

- ✓ Business plan,
- ✓ Strategies (eg international, communications, exercises etc)
- ✓ Resource Planning
- ✓ Performance Management
- ✓ Business enablers like IT and knowledge management.
- ✓ Training and Events

Knowledge

- ✓ Physical
- ✓ Personnel
- ✓ Information
- ✓ Threat Assessment
- ✓ Advisories – CERT plus

R and D – as an under-pinning activity

What are the main security research areas?

- ✓ Electronics and control systems (e.g. detection and vision systems, access control, multi-sensor networks, in-vehicle systems, intrusion detection, SCADA, next generation networks, ATN, Inter-dependencies, RF/DEW (as required))
- ✓ Structural (e.g. ballistics & blast, **physical barriers**, locks, containers & doors, design, air flow systems)
- ✓ Screening & Detection (explosives, weapons, CBRN, including epidemiology)
- ✓ Human Factors (biometrics, behaviour, radicalisation, 'insider threat', design of systems, prophylactics & countermeasures)

Concerns about sophisticated eAs

- Increasing number of co-ordinated, sophisticated eAs targeting HMG, individuals & industry sectors
- Trojans major method to introduce malware into IT systems
- eAs undertaken by range of threat groups ... some with extensive resources
- eAs exploit richness of software, connectivity, lack of user awareness:
- Detection remains patchy ...
- May be impossible to mitigate without new IT architectures

Exploiting Cyberspace: summary of concerns

- Social division, cultural understanding, language
- Technological determinism
- Organised crime
- Situation awareness
- Defence in depth vs. deperimeterisation
- Exponential growth, convergence & pervasiveness
- Complexity of R&D requirements
- Don't just think outside the box...forget the box.

What does CPNI Deliver?

Product Leadership Organisation



How does CPNI Deliver?

Delivery may be

- ✓ One to One
- ✓ One to Many
- ✓ One to All

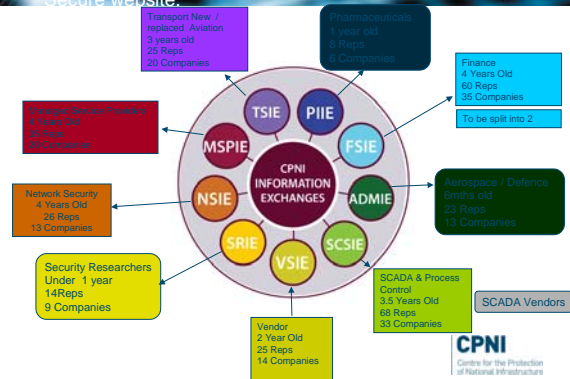
CPNI
Centre for the Protection
of National Infrastructure

One to One

- ✓ Site visits
- ✓ Assurance reports
- ✓ Tailored advice

CPNI
Centre for the Protection
of National Infrastructure

One to many: Exchanges, Conferences, workshops, training Secure website.



Working with CPNI Enables Risk Management

Trusted Networking

- ✓ Discuss with peers in a 'trusted' environment.
- ✓ Confidential briefing using traffic light protocol and protective marking
- ✓ Issues for escalation carry the authority of a trusted Government source.
- ✓ Trusted sharing across business sectors eg through conferences for Exchanges.

Threat Validation

- ✓ Issues validated or discredited.
- ✓ Where genuine threats are discovered and reported, CPNI provide an expert view

Early Warning

- ✓ Advice on new vulnerabilities and mitigating actions

Best Practice

- ✓ Practical advice about how to minimise security risks

CPNI
Centre for the Protection
of National Infrastructure

CESG

- ✓ CESG provides IA advice, products and services to Government and the public sector.
- ✓ CPNI provides integrated physical, personnel and information security advice and products to the CNI and physical and personnel security advice to Government and the public sector. Where integrated advice is required by Government...CESG and CPNI work together.
- ✓ CESG provides technical expertise to support CPNI work with the CNI
- ✓ CESG and CPNI share visibility of...their activities...

CPNI
Centre for the Protection
of National Infrastructure

Framework Programme 7

Security: €M 1400

ICT: €M 9050

- Security and Trust in dynamic and reconfigurable service architectures.
- Identity Management & Privacy enhancing Tools
- Trust Policies
- Trusted computing infrastructures ensuring interoperability and end-to-end security of data & services
- Security and dependability in the engineering of software and service systems

Coordination Actions


SecurIST : (www.ist-securist.org) security projects cluster


ESFORS : (www.esfors.org) security forum for s/w, services

CI2RCO (www.ci2rco.org) critical information infrastructure protection

<http://cordis.europa.eu/fp7/dc/index.cfm>

Keywords: IRRIS, CRUCIAL, GRID.







One to all - New CPNI Website www.cpm.gov.uk **CPNI** Centre for the Protection of National Infrastructure

What we do
Our advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services delivered for the communications, emergency services, energy, financial, food, government, health, transport and water sectors safer. Without these services, the UK could suffer serious consequences, including severe economic damage, global media disruption, or even large scale loss of life. CPNI which is targeted primarily at the critical national infrastructure (CNI) which are the backbone of the national infrastructure which are crucial to the continued delivery of essential services to the UK.

What's new
1 February 2007
CPNI, launched on 1 February, is the Government authority which provides protective security advice to businesses and organisations across the national infrastructure. CPNI has been created by the merger of the National Security Advice Centre (NSAC) and the National Infrastructure Security Co-ordination Centre (NISCC).

Top ten security guidelines
The following is a summary of our ten protective security tips:

- assess the risks to your business
- consider security first when planning building works
- establish a security culture in your business
- keep premises clean and tidy
- control access points and use staff and visitor passes
- install physical measures (e.g. locks, alarms, CCTV, lighting etc)
- establish good mail handling procedures
- recruit carefully, checking identities and following up references
- take proper IT security precautions
- test your business continuity plans regularly

VeriSign

DRDC-ONSA
Ottawa, 23 Mar 2007

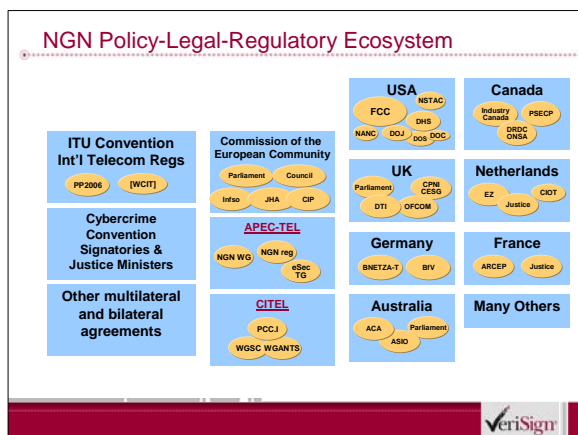
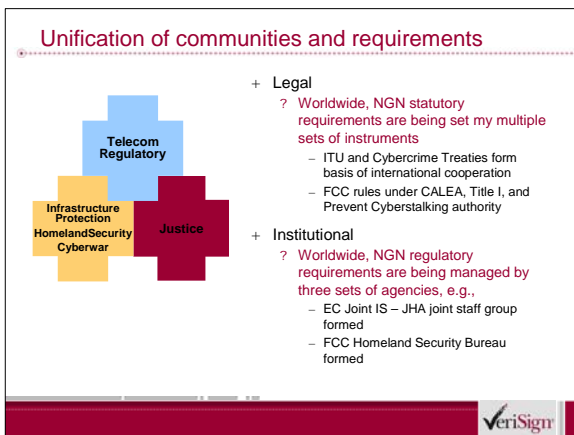
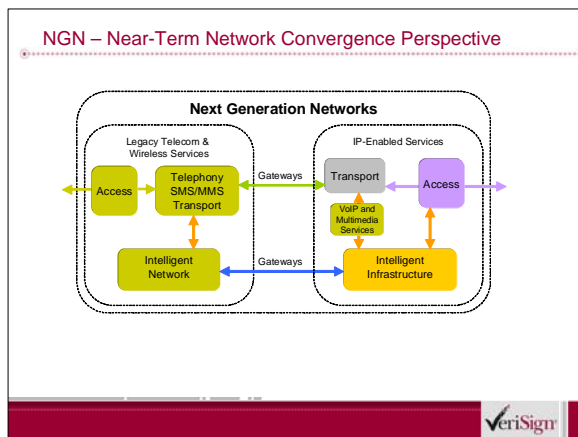
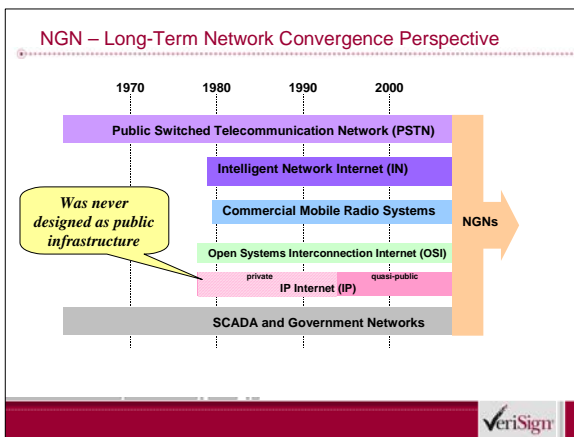
Protection and Other Mandates for Public Infrastructure : Synergies and Globalization

Tony Rutkowski, VeriSign
VP Regulatory Affairs and Infrastructure Standards
Member, FCC Commercial Mobile Service Alert Advisory Committee
mailto:trutkowski@verisign.com

Where it all comes together.

Overview

- + At a high level, large numbers of organizations and activities worldwide are all focussed on Next Generation Networks
- + The result is a common set of technical requirements and government mandates such as infrastructure protection and NS/EP
- + The necessary capabilities have substantial synergies in supporting those mandates
- + *Identity Management* in the broadest sense emerges as the most important capability for these Next Generation Networks
- + Significant diverse global work is now ensuing on Identity Management in a great many forums
- + A common global framework for Identity Management is now being nurtured in some ITU-T forums, especially the IdM Focus Group
- + The threshold for involvement is low, and significant R&D needs exist



Cybercrime/Cybersecurity Norms

- + Kyiv Conference, 6-7 Feb 2007
 - ? Council of Europe and the European Commission support Ukraine as followup to Cybercrime Convention ratification
 - ? CoE Sec-Gen statement regarding child predators in cyberspace and Convention being open to additional signatories
- + ITU Plenipotentiary Conference (Antalya, 2006), SPU
 - ? RES 71 Strategic plan for the Union for 2008-2011
 - ? RES 130 Strengthening the role of ITU in building confidence and security in the use of information and communication technologies
 - ? RES 149 Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies
 - ? SPU global updates www.itu.int/osg/spu/cybersecurity/pgc/
- + Infrastructure Protection Initiatives
 - ? EPCIP – European Programme for Critical Infrastructure Protection
 - Activity led by Directorate-General for Justice, Freedom and Security (JLS)
 - ? APEC TEL/SEC ISTWG + SCADA
 - ? USA NSTAC programme on CIP
- + Analytical capabilities becoming commercial offerings
 - ? VeriSign **iDefense** services



NGN common infrastructure requirements worldwide

- + Availability, security, and legal
 - ? Maintaining high availability, minimizing outages; services restoration
 - ? Priority access capabilities
 - ? Assistance to law enforcement (LI, data retention, cybercrime mitigation)
 - ? Public Safety (E911, emergency alerts)
 - ? Digital rights management
- + Competition
 - ? Unbundling
 - ? Interoperability
 - ? Nomadcity (number portability, roaming)
- + Operations
 - ? Identity Management
 - ? Inter-carrier compensation
 - ? Billing and accounting
- + Consumer
 - ? Universal service
 - ? Preventing intrusions (DoNotCall, CallerID)
 - ? CPNI protection and privacy
 - ? Disability assistance
 - ? Fraud management



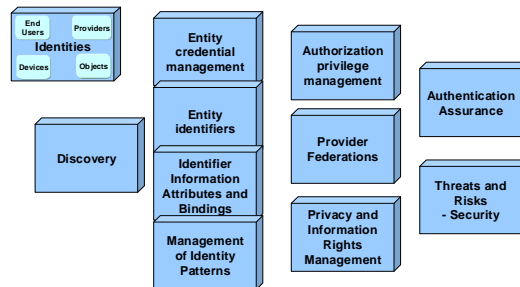
Mission of the International IdM Initiatives

- + Originated with NSTAC NGN Focus Group consensus that Identity Management was a critically important infrastructure capability that includes
 - ? Common global ability to
 - Rapidly discover and query authoritative source information for any entity's*
 - identities, credentials, identifiers, communication routing, attributes, and patterns for any entity involved in a communication
 - Use an assurance trust metric and protocol associated with all identities and identifiers
- + Requires
 - ? Convergence on discovery and interoperability capabilities
 - ? Accommodation of platform diversity and autonomy
 - ? Extensibility to enable constant evolution

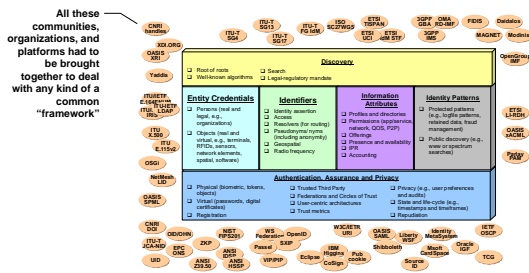
* "Entity" includes "anything that has separate and distinct existence that can be uniquely identified" (real persons, legal persons, objects, geospatial constructs, RFID, sensors, devices, software,...)



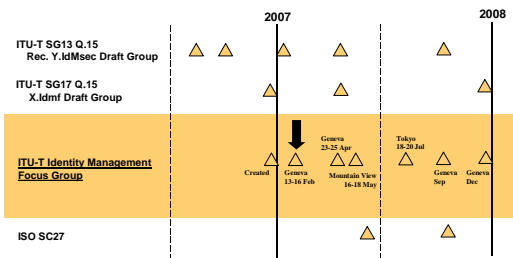
Identity Management Building Blocks and Scope



The Challenge: IdM Ecosystem divergence



The Identity Management Global Venue Timetable



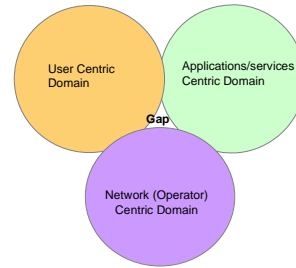
ITU-T IdM Focus Group Basics

- + Established ITU-T SG 17 for one year
 - ? Chair – Abbie Barbir (Nortel)
 - ? Vice-Chair – Richard Brackney (DoD)
- + Open to non ITU-T members
 - ? Proactive outreach to stakeholders from a wide range of areas – web services, NGN, user-centric identity and other SDOs were invited
 - ? Included highly active Identity Management developer community
 - Identity Commons
 - OpenID
 - Identity Gang
 - Windows CardSpace
- + Work conducted using mix of unstructured (OpenSpace) and structured legacy ITU-T standards meeting processes
- + A Wiki was established to allow for continuing autonomous group interaction and inputs and consensus building
 - ? <http://www.ituwiki.com>



Consensus on Nature of the IdM Gap

- + Current state of IdM is that it is being viewed and addressed in a disconnected manner (i.e., silos) from the following perspectives:
 - ? User-centric perspective (e.g., capabilities to allow user control of personal identifiers, roles and privacy attributes)
 - ? Applications/services (e.g., applications and services developers)
 - ? Network (e.g., service and infrastructure providers)
- + Each domain is being independently developed for specific near-term / first-to-market needs, without consideration for the value/need for interoperability and harmonization.



Consensus on Potential Interoperability

- + Gaps are related to the exchange, correlation and linkage of the identity related information between the different planes (user, application/service and network)
- + Includes
 - ? Data model for exchange (pull and push) of identity related information between the network and application/service (e.g., application requesting and the network providing location or network address information as generic objects)
 - ? Architectural model to allow correlation of the identity related functions in the different planes (e.g., user control process, application process and network functions) to allow interoperability (i.e., bridging of existing functions and capabilities) and adherence to policy controls
 - ? Model to support user control of certain network related preferences (e.g., user control of network/service provider preferences and privacy attributes)



Cyberprotection operational use case

- + As IdM capabilities and services begin to be supported by the public and enterprise network infrastructures, both end users and service providers will continue to be subjected to cyber attacks, as well as attacks specifically focused on IdM systems, capabilities and services as they are deployed.
- + Scenarios include
 - ? Use of IdM capabilities to identify, protect and respond to cyber attacks generally
 - ? Response to attack on IdM infrastructure itself

From Telecordia IdM EG Doc.



Value of IdM Information Sharing and Coordination

- + Significant value for the attacked service provider to share information and coordinate across its enterprise and with other services providers and/or government / industry Information Sharing and Analysis Centers (ISACs) and Computer Emergency Response Teams (CERTs) both nationally and internationally, in a trusted manner
 - ? to determine if an attack is focused or broad-based, and if other service providers have IdM elements that affect the attacked service provider necessitating action to partition off the attack
 - ? Attacked service provider should provide other service and network providers attack information to check if they are affected and prevent propagation of attack vector
 - ? Coordination may leverage existing cyber security coordination mechanisms, or may require new coordination procedures
- + IdM capabilities can be leveraged to facilitate rapid coordination and sharing of information based on pre-established and authenticated trust relationships
 - ? a separate trusted database can be created that coordinates information regarding IdM related cyber attacks
 - ? Allows coordinated sharing and response
 - IdM can be used to authenticate responding service providers and ISACs / CERTs
 - use IdMs to authenticate Network Elements to validate relationships between network elements to ensure the legitimacy of the transactions



International IdM Public R&D/Standards Initiatives

- + European Union R&D Consortia
 - ? 6th Framework Programme 2002-2006
 - Daidalos (www.its-clusters.org)
 - Focused on network IdM platforms
 - GUIDE (
 - Focused on a conceptual framework for eGovernment IdM
 - Modire (www.csis.eur.nl/kuboven/belvedere.htm)
 - Focused on eGovernment IdM in the EU pursuant to the i2010 plan
 - PRIME (www.eugma-project.eu)
 - Focused on privacy-enhancing Identity Management Systems
 - ? 7th Framework Programme 2007-2008
 - €9.1 billion for funding ICT
 - FP7-ICT-2007-1: Objective ICT-2007.1.4: Secure, dependable and trusted Infrastructures
 - Identity management and privacy enhancing tools
 - FP7-ICT-2007-1: Objective ICT-2007.1.6: New Paradigms and Experimental Facilities
 - trust and identity management architectures and technologies
- + European Union Standards
 - ? ETSI Specialist Task Force QZ on Security and IdM in NGN
 - Permanent expert staff to facilitate and develop standards-based IdM solutions
- + Korea
 - ? ETRI (http://www.etri.re.kr/www_05/e_etri/)
 - Focused primarily on IdM of RFID and objects under the aegis of Network Identity (NID)
 - Coordinating Japan, China, and Switzerland on NID



Recommendations

- + IdM Focus Group provides unique opportunities to discover and analyze new IdM developments, participate, and shape global IdM infrastructure capabilities
 - ? Includes an enormous array of well-funded IdM R&D activities worldwide
 - ? Valuable to CIP and entire associated NS/EP community and industry
 - ? Opportunity to work directly with counterparts in other regions and countries
 - ? Builds directly on the Ottawa NSTAC 2006 RDX Workshop
- + Impediments to participation are minimal
- + R&D, analyses, and inputs are especially needed for CIP and NS/EP related IdM capability requirements
- + R&D topics available at
http://www.ituwiki.com/index.php?title=IdM_Annex_Topics



Annex 5 -- Working Group Notes

Cyber A – Communications

Summary

Trends

- Outsourcing core (mission critical) software
- Meshed sensor networks
- Ubiquitous networks
- Humans will remain a vulnerability
- Increased physical threads (interconnects)
- Increased cyber warfare (overt & covert)
- Identity becoming more important (passports)... Human \leftrightarrow machine and machine \leftrightarrow human

Threats

- Malicious code
- Integrity, availability, confidentiality
- Complexity (inherent) – no one knows how to fully secure this – identity theft
- Exploiting social engineering
- Physical threat from cyber connectedness
- Massive loss
- Identity theft and misuse

S&T Capability

- Detection of malicious code/reverse engineering
- R&D in security in sensor networks (sensor, transmitting device, net)
- Mobile *ad hoc* networks security / security in protocols/standards / identity management
- Model and profile human motivation/vulnerabilities
- Inventory physical nets/deal with differential protective incentives
- Offensive measures investments (deception/decoup/intrusion/synthetic environments/weapons effects, etc.)
- CNO – identity management/authentication/authorization

Other – Non-S&T

- Change policy to minimize insertion of malicious code
- Policy of use
- Something to deal with liability
- Educate, train, policy
- Institutional – linkages with diverse owners/operators to be prepared for attacks/scenarios
- Prepare for and address legal and ethical barriers –new legislation required

Detail

1. World/Context 2020 – (quite predictable, few responses ready)

- **Vast increase**¹¹ in cyber entities/object $\leftarrow \rightarrow$ transactions/human $\leftarrow \rightarrow$ institutional dependency/ubiquity/vulnerability
- New, capable **leadership from Asia**
- **Power of non-state** actors increasing/increased global economic disparities
- Threats are against private and public, but *intelligence* (espionage, crime, hacking) is largely public \rightarrow need for new collaborative models of trust, institutions
- **Offensive measures** possible/needed (Big Brother router/reader/intervener?)
- **Wild cards possible** – will create major shift
- By 2020 these problems not all likely to be solved
- Economies do drive toward centralized systems of certain functions and decentralize others (distributed cyber – centralized security?)
- Open source/free market access (e-Bay ++) = increased value and vulnerability outside state control

2. Cyber Issues/Drivers/Threats/Vulnerabilities

- **Identity (individual and agent)/authentication/agile** but trusted management protocols
- Complexity management/institutional/object based
- Detection/attack and outage reporting/**interagency collaboration and organization/intelligence**
- Integrity of systems/trust mechanisms/Quantified degrees/context for trust, relationships
- Development of mobile/voice/biometrics/avatars/virtual life economy
- Hoax/hysteria (**SCADA machine agents**) magnified power of BIG
- Training/awareness/institutional learning
- Cyber law/international policing and prosecution
- Offensive measures
- Intent migration towards sensor net

3. Response Strategies

Hazards & Vulnerabilities “Back in 1800”

- Financial transactions
- Health information and identity theft
- Public confidence in P&P systems
- Compromised security infrastructure and capacity
- Personal safety (e.g. in winter) transport
- Viability of food/health systems (seniors)

Assumption: By 2015 there is a more systematic way to manage this spectrum

¹¹ Bolded elements were identified by team as key references for summary

↓

PREVENT	PREPARE	MITIGATE/REACT	RECOVER/ADAPT
<ul style="list-style-type: none"> • Awareness of vulnerabilities • Plan and coordination of capacities • Review public-private motivation for security incentives 	<ul style="list-style-type: none"> • Military and civil scenarios/actions (regularize) • Redundancy of systems • Simulation and modeling (build) and exercises (deploy) 	<ul style="list-style-type: none"> • TCP/IP evolution path – moving towards increased security, will cost \$billions to replace 	<ul style="list-style-type: none"> • Institutionalized lessons learned • First responders – crisis management and communication • New members CBRN/cyber logic

- Offensive measures (e.g. disconnect to threat sites/isolation) (reciprocal attacks/warrior training +)
-

<ul style="list-style-type: none"> • Assumption: New first response profiles/skills and organizational development • Proactive national security infrastructure in place by 2020 • Assumption: Math for complexity readiness security • Modeling 	<ul style="list-style-type: none"> • New institutional trust mechanism • Sharing vulnerability and attack information • New IP protocol with enhanced security • Quantified differential levels of trust (algorithms and protocols) • Human skills – management, policy • Communications, national plans, key regulations, IP, crisis management • Law Enforcement Agencies ready to deal with • National warning and authentic systems – mesh-working 	<ul style="list-style-type: none"> • Social net – threat patterns, studies – social engineering • Incident strategy – typology for public (commercial and technical) 	<ul style="list-style-type: none"> •
--	---	--	--

4. S&T Capabilities

- Proactive role to preserve integrity/trust role with US and UK
- Scanning/trends/inter-operative capacities in security technologies and architectures
- Algorithmic development for trust/authentication/intelligence/human behaviours & motivations

- Change silos paradigm (Cold War) to improve institutional collaboration
- Mapping of cortical IP/infra/system assets (to defend) physical +
- Knowledge map of intangible/tacit assets/exposures – e.g. domain name directories/people assets
- National business/government services continuity plans and policy based (management of relationships) network management capability
- National detection/alert/warning system
- Advanced detection/tracking/traceability/tags (nano/micro/molecular) and embedded information links and interpretation
- Digital mesh sensor networks
- R&D in sensor nets for security (components, etc.)
- Malicious code detection/re-engineering
- Mobile ad hoc network security
- Identity management/authentication/authorization

Cyber B – ICT infrastructure for Transport, Finance & Power Distribution

Q 1 – Threats

- All systems highly cyber dependant
- Threat environment is much worse in 2015
 - System complexity
 - Demands and reliance on critical infrastructure
 - Intelligence increases
 - Wild weather
 - Security
 - SCADA
- Number of attacks and the good guy/bad guy knowledge gap increase
- Number of ways
 - Nation/corporate disruption
 - Asymmetric attacks
- Software reliability
- Sensor networks
- Information availability

Q. 2 – Ideal World Responses for Threats

- Self-healing IT systems
- Maintaining redundant systems
- Interdependency of interconnected systems
- Evaluation of accuracy of data for open models
- Total defence resilience
- Private WIKI intelligence
- Software assurance
- Red teaming
- Formal methods for software (total ICT security \$300 million)
- S supervisory control and data acquisition (SCADA) vulnerability – “Achilles Heel”
- Redundancy for smart threat
- Warning
- Safety/insurance

Q. 3, 4 & 5

1. Modeling – interdependency
 - Predictive
 - Real-time
 - Cost/benefit
 - Risk analysis
2. Software assurance – government leads
3. Formal methods
 - Secure development life cycle
 - Embedded systems
4. Self-defending systems
5. Sandboxing
6. Sensors for unanticipated events
7. Self-organizing, traffic systems
8. URGENT – SCADA vulnerability detection technology
9. Secure SCADA

Key Insights and Conclusions

- Improve warning
- Incremental improvement to networks and their security
- Improve analysis of risk and vulnerability
- Incremental improvement to network defence capability
- Increased collaboration to improve information and intelligence
- Cooperation required with entire communities.

Human Infrastructure

Summary

- Augmented collaboration
 - Wiki, cognitive sciences → group
 - Sociology, anthropology, communications theory
- Augmented cognition
 - Modeling and game theory, cognitive sciences, epidemiology, data-mining, human-machine interface
- Preparedness exercises
- Cultural integration & cross-cultural¹² communications

Detail

Defining the Risk

Centre of Gravity:

- Public confidence
- Threats to "social and national resilience"
- Social trust
- Market trust
- Government trust
- Networking/Wiki structures vs. centralized command and control

ADAPTABILITY

Virtue of Distrust:

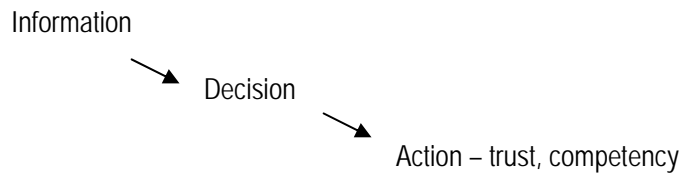
- Engenders a readiness to try other solutions (don't rely on authorities)

Trust in Government

- Precious – if you've got it, preserve it

Mismatch between nature of the problem and command/control structure

¹² Culture within organizations as well as ethno-linguistic communities



Weak points of decentralized systems:

- The Press – exacerbates breakdown of trust – command and control of news

Strong points:

- Wikipedia – costless self-organization – new Fifth Estate

Role of abstract vs. concrete measures

Source of Threat

- Those who feel disempowered or extremists
 - Aboriginal groups
 - Eco/environmental groups
 - Insiders
- Catastrophe is enabled by failures of preparedness, which may be taken advantage of by extremists
- Communities may be traumatized for years by events of little national significance; national response must percolate down to right level of granularity
- Emergency circumstances are behaviour drivers – long-term cascade effect on people's behaviours

Remediation:

Example: first nations activism – partly solved through education/outreach

Canada 2020

- Increasingly customized view of the world
- Degradation of single national consciousness previously provided by mass media
- Mass media used to frame issues/facts in a way that became common to all – how to preserve that? Google?
- How to understand how we do it now, and how to maintain a positive direction

Next steps:

- Apply these questions to our four problem domains
 - Look for framing/defining events... eg. Kennedy, 9/11
-

Outline of 2020

- Telecoms the glue for all sectors – vulnerable point for all
- Natural/accidental most likely
- Intentional most dangerous both physically and dangerous to trust

Example: recent refinery fire/gas shortage. Human failures of planning, communication, mass response, etc.

Idea: reframing infrastructure as a capability

- Networked individuals/groups have many more loose connections to other nodes, which increases knowledge (Al Queda meets IRA, Bob meets Xiolin) Increasing “splintering” or granularity to social “tribes”.
-

DANGERS 2020

- Anti-microbial resistant diseases
 - Re-emerging old pathogens (drug-resistant syphilis)
 - New diseases (SARS)
 - Man-made chimeras

 - Convergent factors – climate change, urbanization, democratization
 - Global mobility
 - Anonymity vs. privacy
 - Increasing numbers of people with advanced degrees in hard sciences
 - Increasing specialization leading to less redundancy
 - Rigid occupational structure
 - Too much interconnectedness leading to vulnerability of total system to “sand pile collapse”
 - Demographic shift – dependency on immigration – screening critical workers
 - US/Canadian cross-border issues
 - End of English language hegemony
-

- Currency control in an age of borderless e-commerce – failure of cash economy in crisis
- Increased militancy of home-grown groups
- First nations
- Environmentalists
- Anti-globalists, rural interests
- Disaffected youth
- Xenophobic reactionaries
- Increased militancy of imported groups/cultures
- New transport/energy systems bring unforeseen dangers
- Climate change disruptions
- Arctic security/sovereignty issues due to opening of Northwest Passage
- Reduced redundancy – reducing surge capacity, e.g. in finance sector with increasing numbers of daily transactions
- Organized crime, e.g. in oil sands region – rapid response of mafia to populations made vulnerable by disaster
- Dependency on strategic west coast ports
- Lack of authenticity of news – phishing and misinformation
- Labour strife in critical services
- Corruption
- Business/union turf wars
- Inadequate training for rare catastrophic events (Homer Simpson manning the switch)
- Multi-agency preparedness – lack of inter-agency collaboration
- International drivers of our standards

SOLUTIONS

- Assured representation in international bodies in standards, protocols, rules of trade
- Sociology of immigrant integration/removal of barriers to immigrant integration
- Preparing/educating people for preparedness; funding for preparedness exercises (SimCanada)
- Enable a small number of people to securely and sustainably support critical systems in emergencies
- Risk education and risk communication/desensitization
- Redundancy/surge capacity (e.g. during market failures)
- Technology and processes to support timely collaboration among stake-holders
- Man-machine collaboration and modeling (SimCanada)
- Community preparedness/empowerment
- School-level public education in preparedness
- Human life-cycle management for a population that now lives 100+ years
- Data mining/modeling – small-signal event modeling

- Systems bypass
 - Credential validation/authentication of messages/news
-

- Peer production (wiki-security) e.g. of knowledge; systems in support of mentoring
- Studies for multi-traditional collaboration/interest convergence/augmented collaboration
- Organizational anthropology
- Operations research
- Cognitive psychology – information imaging and framing technologies
- Artificial intelligence/augmented cognition; digital humanities
- Gaming
 - Modeling and simulation
 - Community dialogue and collaboration skills – sharing of information
 - **Game theories** – neo-détente, or multi-polar détente
- Real-time epidemiology – contact tracking, real-time molecular epidemiology
- Complexity science
- Medical/research disciplines – e.g. nano-medicine, antibiotics

Physical Infrastructure

PHYSICAL INFRASTRUCTURE

COMMUNICATIONS	TRANSPORTATION	ENERGY DISTRIBUTION	FINANCE
<ul style="list-style-type: none"> Cell towers Fibre lines/cabling Satellites and receivers/dishes Processing facilities/buildings Cells/wireless/wired devices Transmission sites Crisis management buildings TV/Radio 	<ul style="list-style-type: none"> Rail lines Stations Bridges/tunnels Ports/ships Locks Aircraft Airports Roads/buses Seaways Urban infrastructure Key intersections 	<ul style="list-style-type: none"> Pipelines – oil, gas, CO2 Transmission grid Transport of energy Gas/H2 stations (more local Canadian infrastructure in 2020) <p style="text-align: center;">↓</p> <ul style="list-style-type: none"> Significant ripple effects to other sectors 	<ul style="list-style-type: none"> ATMs Physical infrastructure Banks/Credit Unions Distribution of money Processing centres Production facilities – money and credit cards TSX building, etc.

CRITICAL THREATS TO PHYSICAL INFRASTRUCTURE

COMMUNICATIONS – CRITICAL THREATS

Intentional

P-1 XX	EMP (non-nuclear)
P-2 XX	Destruction – or the threat of destruction – of physical infrastructure (e.g. explosion)
P-3 XXXXX	Denial of physical access (e.g. anthrax)
P-28 XXX	Lots of “new” stuff (including business models) = more vulnerabilities

Accidental

P-17 X	Destruction
P-4 XXXXXXXX	Systemic Interconnectivity - cascade
P-5 X	Human Error
P-6 XX	Design fault
P-7	Cost-cutting/lack of incentives

Natural *(all more severe in 2020)*

P-8	Lightening strikes
P-9	Ice storms
P-10	Wild fires (increasing x 2)
P-11 X	Landslides
P-12	Tsunami +++
P-13 XXXXX	Extreme weather (increasing)
P-14	Earthquakes/volcanoes
P-15 X	Poles reversing
P-16	Solar storms

TRANSPORT – CRITICAL THREATS

P-1 – P-17	All of the Intentional, Accidental & Natural threats listed above
P-18 XXX	Intentional/natural congestion
P-19 X	Minefields - ports
P-20 X	Blockage of evacuation routes
P-21 XXXX	Vulnerability is “jurisdictional cracks”
P-22	<u>Accidental</u> denial of rail/marine/air service
p-23	Attack on Air Traffic Control

ENERGY DISTRIBUTION – CRITICAL THREATS

P-1 - 17	All of the Intentional, Accidental & Natural threats listed above
P-24	Jurisdictional threats
P-25	Fuel contamination (accidental or intentional)
P-26	“Rust Out”
P-27 XX	Permafrost melting e.g. damage to northern pipelines, transport problems
P-30 XX	Deliberate sabotage to power distribution system

FINANCE – CRITICAL THREATS

P1-28	All Intentional, Accidental & Natural plus most of Energy
P-29	Huge devaluation of physical assets, e.g. lack of access to mines/environmental change of valuation
P-31 XXXXX	Higher reliance on cyber for financial transactions in 2020

ACTIONS TO STOP OR PREVENT RISKS IN ALL SECTORS

P-4 Systems Interconnectivity – Cascade Effect

BEFORE	DURING	AFTER
<ol style="list-style-type: none"> 1. Modeling new/existing and better design of complex, robust systems for prevention and emergency planning 2. Identify critical hubs in system 3. Take steps to protect information in steps 1 & 2 4. Include systems management approach in the modeling 5. Prepare robust threat and management process and plan 6. Practice responses in advance (exercises) and apply learnings 7. educate public on all roles 8. Confirm human and technological robustness 9. Build in appropriate redundancy 10. Prepare directory of responsibilities (see also P-21) 11. Realistic risk assessment of these cascade events 12. Good early warning systems 13. Common operating picture among the key sectors 14. Independent redundancy communications among first responders 	<ol style="list-style-type: none"> 15. Fast response to detection systems (automated) 16. Implement good consistent communications plan (public, responders, media) 17. Good situational analysis/awareness 18. Ability to resort to low-tech solutions 19. Implement data-logging 	<ol style="list-style-type: none"> 20. Review data logging → for lessons learned ↓ 21. Loop back to implement plan improvement and model updates 22. Manage public perception 23. Business resumption plan (clean up, re-start, repair & rethink) ↑ 24. Implement lessons

P-1 & P-2 Explosion/Destruction of Physical Infrastructure – Accidental or Intentional

BEFORE	DURING	AFTER
<ol style="list-style-type: none"> 1. Identify priorities to harden based on threats/risks 2. Better people surveillance, detection, monitoring 3. "Harden" the physical infrastructure (multiple techniques) 4. Prevent attacks through good Intelligence 5. Eliminate some physical infrastructure 6. Reduce visibility of critical infrastructure 7. Distribute critical infrastructure (more difficult to attack/less impact) 8. Hostile intent detection (disparate information sources) 9. Tools for detecting devices 	<ol style="list-style-type: none"> 10. Fast response – isolate to limit impact/cascade <ul style="list-style-type: none"> • Fast response • Auto/manual • Robust 11. Implementation of multi-faceted plan – e.g. hazardous materials 12. Forensic analysis 13. Triage 	<ol style="list-style-type: none"> 14. Identify "bad guy" <div style="text-align: center;"> ↓ Find "bad guy" ↓ Rectify </div>

P-5 Human Error¹³

BEFORE	DURING	AFTER
25. Modeling new/existing and better design of complex, robust systems for prevention and emergency planning 26. Identify critical hubs in system 27. Take steps to protect information in steps 1 & 2 28. Include systems management approach in the modeling 29. Prepare robust threat and management process and plan 30. Practice responses in advance (exercises) and apply learnings 31. educate public on all roles 32. Confirm human and technological robustness 33. Build in appropriate redundancy 34. Prepare directory of responsibilities (see also P-21) 35. Realistic risk assessment of these cascade events 36. Good early warning systems 37. Common operating picture among the key sectors 38. Independent redundancy communications among first responders 39. identify priorities to "harden" based on threats/risks Balance 40. Better people surveillance, detection, monitoring 41. Eliminate some physical infrastructure 42. Reduce visibility of critical infrastructure 43. Distribute critical infrastructure (more difficult to attack/less impact)	44. Fast response to detection systems (automated) 45. Implement good consistent communications plan (public, responders, media) 46. Good situational analysis/awareness 47. Ability to resort to low-tech solutions 48. Implement data-logging	49. Review data logging → for lessons learned ↓ 50. Loop back to implement plan improvement and model updates 51. Manage public perception 52. Business resumption plan (clean up, re-start, repair & rethink) ↑ 53. Implement lessons

target harder to get at than accidental/intentional

¹³ Ken – your notes showed P-5 as containing all of P4 + - but it was unclear if you were referring to all of P1/2 or just to bits that were in pink?

Q. 3 CRITICAL SCIENCE TO SUPPORT/ENHANCE ACTIONS

(All of these are interconnected and have impacts back and forth (feeding/receding))

MATHEMATICS XXXXX	<ul style="list-style-type: none"> • Systems design (engineering) • Network theory • Optimization • Risk measures/decision rules • Modeling • Encryption • Non-linear systems
PSYCHOLOGY XXX	<ul style="list-style-type: none"> • Implementing lessons learned (responders) • Crisis management • Public, responders, planners, instigators (accidental/criminal) • Perceptual (seeing the most important stuff) (browse)
HUMAN RESOURCES/BEHAVIORAL SCIENCE X	<ul style="list-style-type: none"> • Management sciences • Reactions under stress/pressure • Emotional intelligence • Training skills/science
COMPLEXITY SCIENCE XXXXX	<ul style="list-style-type: none"> • Biological systems • Design for resilience • Inter-organization coordination • + Murphy's Law • + Adaptive and evolutionary strategies
ARTIFICIAL INTELLIGENCE (AI)	
EDUCATION X	<ul style="list-style-type: none"> • Skilled resources to: <ol style="list-style-type: none"> a. Create all the above b. Use it

ADVANCED COMMUNICATIONS TECHNOLOGY	<ul style="list-style-type: none"> • Linking first responders • Pervasive wireless
EARTH SCIENCES XX	<ul style="list-style-type: none"> • Geophysics • Environmental science • Weather prediction and climate impact modeling
PATTERN RECOGNITION	<ul style="list-style-type: none"> • Flow of physical objects
MATERIALS SCIENCE/ARCHITECTURE XXX	<ul style="list-style-type: none"> • Reduce risk of destruction <ul style="list-style-type: none"> ○ “Hardening” ○ Violent threat ○ Natural ○ Criminal • Self cleaning vs. contamination • Smart materials – sensor, warn – real-time management • Environmentally friendly
NEURO-PSYCHOLOGY X	<ul style="list-style-type: none"> • Predicting behaviour <ul style="list-style-type: none"> ○ Enemy ○ Responders ○ Human error/operators ○ Prevention ○ Treating
IDENTITY MANAGEMENT OF PHYSICAL OBJECTS	<ul style="list-style-type: none"> • Detect changes • Embedded detection of problems • Authentication
QUANTUM PHYSICS	<ul style="list-style-type: none"> • Beam to change behaviour? (hi-tech lobotomy) • Quantum computing (speed and efficiency of processing)

<p>URBAN PLANNING/INFRASTRUCTURE PLANNING/CONSTRUCTION</p> <p>X</p>	<ul style="list-style-type: none"> • Threat-resistant • Design for resilience/security
<p>VISUALIZATION/RENDERING OF COMPLEX INFORMATION</p> <p>X</p>	
<p>SPACE SCIENCE</p>	<ul style="list-style-type: none"> • Threat reduction
<p>LANGUAGE/LINGUISTICS</p>	
<p>SCIENCE OF SUCCESSFULLY IMPLEMENTING NEW PHYSICAL INFRASTRUCTURE</p> <p>X</p>	<ul style="list-style-type: none"> • Without experience
<p>FORESIGHT 2020</p>	<ul style="list-style-type: none"> •
<p>ERGONOMICS</p>	<ul style="list-style-type: none"> • Human ↔ machine interface

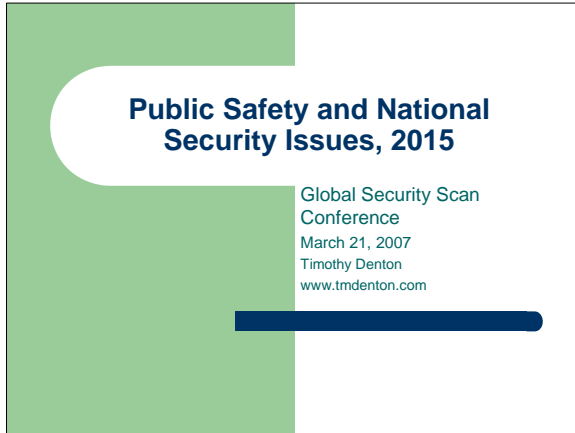
PHYSICAL INFRASTRUCTURE – KEY INSIGHTS

- Recognizing that not **every threat is intentional**/malicious, i.e. most threats are natural or accidental
- Physical infrastructure is very complex and its security will require multiple other sciences and human sciences over and above the sciences/technologies needed to build it
 - **Holistic security ecosystems approach**
 - **Complex inter-dependancy**
- Security strategies must also be **innovative, creative, resilient and economic**
- **Disappearing physical infrastructure** → trend → leads to challenges and opportunities
- **Foresight/scenario evaluations** must be done in the context of the holistic security ecosystem – e.g. epidemiology
- Our technology will have **more interaction = more intelligence on its environment**
- We should **ensure science is also channeled towards interdiction, prediction, prevention, deterrence** – “pre-emptive offensive strategies”
 - Specifically vs. intentional threat
- The **need for low-tech** in a future hi-tech world
- Science solutions must accommodate **combinations of natural/accidental/intentional threats**

Annex 6 -- Additional References

Tim Denton

Public Safety and National Security Issues, 2015



Public Safety and National Security Issues, 2015

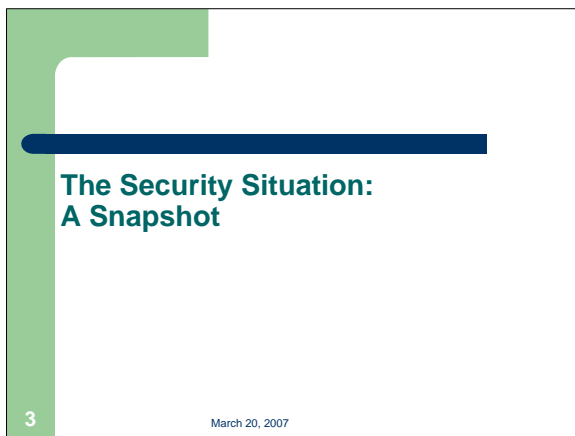
Global Security Scan
Conference
March 21, 2007
Timothy Denton
www.tmdenton.com



What are we talking about?

- Are we dealing with 'security science'?
- or
- Are we dealing with 'science for security'?
- Clearly the latter is more important

2 March 20, 2007



**The Security Situation:
A Snapshot**

3 March 20, 2007



Range of Threats

- Natural hazards
- Major industrial accidents
- Asymmetric events (terrorism)
- State-sponsored espionage
- Industrial espionage
- Criminal & malicious activities

4 March 20, 2007

We need to remember our values

- The open nature of the Internet has allowed *innovation without permission*
 - No one had to ask permission to launch the www or email
- The Internet was created in a high-trust environment of universities and government science projects
- Protecting the cyber-infrastructure means protecting the wealth-creating possibilities of the Internet
- Measures we take should enhance *trust*
 - *Trust is the basis of all collective action*
- Destroy trust and you do the terrorists' work for them

5

March 20, 2007

A Context: Critical Infrastructure

- Ten national critical infrastructures have been identified by the **Department of Public Safety**
- All are interdependent to varying degrees from the need for power to cyber-computer dependencies (Internet infrastructure, DNS)
- Critical infrastructures are a stated target of terrorists

6

March 20, 2007

Problem

- A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures
 - Attacks against .ca and DNS are routine
- The probability of more attacks will likely remain high for years to come
- With each passing year interconnectivity and vulnerabilities increase as does the sophistication of the 'bad guys'
 - As we move to all IP signalling, vulnerabilities may grow
 - Our communications are vulnerable at several choke-points

7

March 20, 2007

Problem 2

- Of primary concern is the threat of organized cyber and physical attacks capable of causing debilitating disruption to Canada's critical infrastructures
- The need to protect these infrastructures is a collective action problem, frequently requiring political as well as collective solutions
 - Individual actors in the private sector may not have the incentive to protect infrastructures to the degree needed.
 - A political and collective solution does not mean a governmental solution: it means all stakeholders must act.
- The appropriate forums will not always be in Canada
 - Standards, such as IP, are international

8

March 20, 2007

How to Address the Problem

9

March 20, 2007

Some General Considerations 1

By 2015 will have in place:

- Traffic flowing through a maze of wireline and wireless routes with a mix of real-time and store-and-forward capabilities
- Widely available 'user-configurable' networking
- Applications that run based on bandwidth on-demand
- IPv6 as the prevailing Internet Protocol

By 2015 we *should* have in place

- Significantly enhanced security within the Internet Protocol (IP), Domain Name System (DNS) & Border Gate Protocol (BGP)
- A comprehensive national plan for securing the key resources and critical infrastructures throughout Canada

10

March 20, 2007

Some General Considerations 2

- By 2015 we should have in place:
 - A national means to provide crisis management in response to attacks on critical information systems
 - Law enforcement capability to deal with cyber threats and vulnerabilities
 - Ability to assess strategic cyber attacks
 - National coordination in providing specific warning information and advice about appropriate protective measures and countermeasures to all relevant organizations
 - An international scheme of authentication that lets us know with whom we are dealing

11

March 20, 2007

Some General Considerations 3

- By 2015 we should have in place:
 - Significantly enhanced awareness by those who need to be in the 'know' regarding cyber security
 - A model of trust that allows sharing of critical information among organizations that 'need to know'
 - A process for national vulnerability assessments to help us understand the potential consequences of threats and vulnerabilities
- The speed with which we accomplish this will depend on how threatened we feel, and from what sources
- How are we going to get this work done, even if we wanted to?

12

March 20, 2007

Future Canadian Cyberspace Needs

- For example, we need to:
 - Prevent cyber attacks against Canada's critical infrastructures
 - Reduce national vulnerability to cyber attacks, and
 - Minimize damage and recovery time from cyber attacks that do occur
 - Strengthen and broaden trusted international collaborations.
- To the extent the vulnerabilities derive from standards (e.g., IP), or are solved by standards, the solutions will not come from within Canada.
- Cyber attacks will be mostly from outside Canada

13

March 20, 2007

Future Canadian Cyber Security Needs

- Monitor, prevent and/or mitigate cyber threats
- Develop 'classified' knowledge map of Canada's cyber infrastructure
- Identify and address known needs and gaps in the knowledge map
- Enhanced system and application interoperability
- Relate international to national developments
 - This requires new models of collaboration among relevant stakeholders
 - The comprehensive view we require will not come from any one actor, sector, or player, but all relevant players

14

March 20, 2007

New Models of Collaboration are Needed

- The institutional response to these problems is vital
- It must allow for private sector leadership where that is appropriate, government influence, and multi-stakeholder representation
- Stakeholders: the cops, the carriers, emergency response organizations, spooks, military, the DNS infrastructure (CIRA), privacy advocates, defenders of the Internet, applications providers (e.g., Google), DN registrars, regulators, whoever shows up
- It must be open to those interested, and probably will contain several sub-assemblies, mini-parliaments, for certain issues
 - ICANN, the Internet Corporation for Assigned Names and Numbers, may provide a model, for or against
 - ICANN runs the DNS, the root servers, the business of registries and registrars

15

March 20, 2007

Institutional Responses

- There is a need for some form of final authority
 - US DoC has authority over which top level domains into the 'root'
- It helps if people see the need to participate
 - Emergency organizations, 9-1-1, carriers, cops
- It helps if organizations can speak to their own interests
 - No need to speak through intermediaries, or governments
- It helps if the structure allows for specialist division of labour
- It is vital that the participants remember that we are trying to preserve innovation, creativity, and the rule of law
 - The goals and culture of the organization should explicitly recognize these points

16

March 20, 2007

Future Canadian Cyber Security Needs 2

- Fund and perform R&D in support of national infrastructure security needs with a view to:
 - gaining new scientific understanding
 - developing new technologies
 - creating new products and systems
 - enhancing national security
 - creating both new wealth & highly qualified people
- Participate in international standards forums where relevant to cyber-security
 - IETF
 - ITU
 - Some solutions will be in the nature of standards, not physical infrastructure

17

March 20, 2007

Future Canadian Cyber Security Needs 3

- Ensure adequate education and training programs in colleges and universities that address national security and national infrastructure security
- Formalize government as an 'early adopter' in defining and satisfying needs in partnership with the Canadian private sector

18

March 20, 2007

2015 - 2020 Requirements


- Ensure consensus among stakeholders as to requirements
 - Some form of stakeholder, parliament/secretariat
 - Let that organization begin to define the requirements
- The problem is how to create an organization, forum or "parliament" (talking-shop) that meets the needs of the interests involved
- The Internet-collaborative model will prevail over centralized and government-directed solutions
- The federal government has a natural and legal interest in the creation of such an organization for cyber-security
- It is a collective action problem for which government was designed

19

March 20, 2007

Robert Lesnewich/ Tony Rutkowski,
*ITU-T Focus Group on Identity Management Report, First Meeting,
 Geneva, 13-16 February 2007, Implications for NS/EP and CyberSecurity
 Operational Response*

V1.4



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
 CSC, Falls Church VA, 7 March 2007

ITU-T Focus Group on Identity Management Report
First Meeting, Geneva, 13-16 February 2007
Implications for NS/EP and CyberSecurity Operational Response

Robert K. Lesnewich, Telcordia
Anthony M. Rutkowski, VeriSign



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
 CSC, Falls Church VA, 7 March 2007

Summary

- The Focus Group meeting was successful as the first global opportunity to get representatives of all of the diverse Identity Management communities together
- Purpose was to gather all the diverse IdM perspectives and gain consensus on
 - A coherent concept of "Identity Management" and various descriptions of constituent components for ICT infrastructure
 - The need for and various descriptions of a common global IdM framework for
 - Discovery of public IdM resources
 - Interoperability among public IdM resources solutions
- The value proposition of continuing open participation in further work of the Focus Group through on-line and F2F meetings over next six months was achieved. See <www.ituwiki.com>
- Compiled information will be made available as a resource for potential recommendations and specifications by ITU-T Study Groups
- Work includes defining and providing for NS/EP and cybersecurity operational needs relating to IdM




ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
 CSC, Falls Church VA, 7 March 2007

Mission of the International IdM Initiatives

- Originated with NSTAC NGN Focus Group consensus that Identity Management was a critically important infrastructure capability that includes
 - Common global ability to
 - Rapidly discover and query authoritative source information for *any entity's**
 - identities, credentials, identifiers, communication routing, attributes, and patterns for any entity involved in a communication
 - Use an assurance trust metric and protocol associated with all identities and identifiers
- **Requires**
 - Convergence on discovery and interoperability capabilities
 - Accommodation of platform diversity and autonomy
 - Extensibility to enable constant evolution

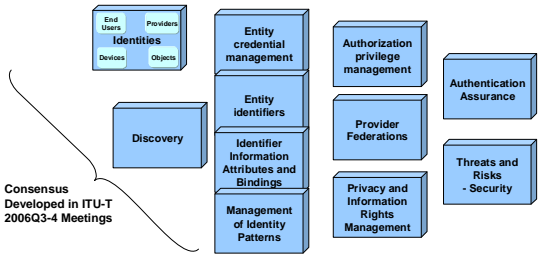
* "Entity" includes "anything that has separate and distinct existence that can be uniquely identified" (real persons, legal persons, objects, geospatial constructs, RFIDs, sensors, devices, software,...)

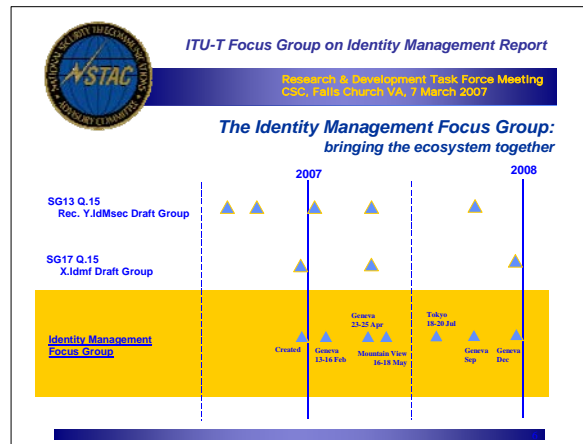
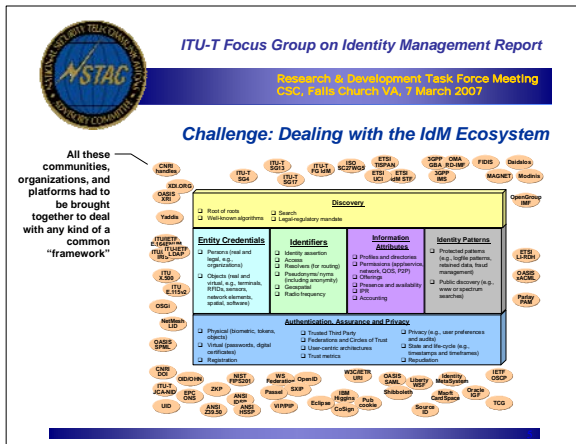


ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
 CSC, Falls Church VA, 7 March 2007

Identity Management Building Blocks and Scope





- ITU-T Focus Group on Identity Management Report**
Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007
- Focus Group Basics**
- Established ITU-T SG 17 for one year
 - Chair – Abbie Barbir (Nortel)
 - Vice-Chair – Richard Brackney (DoD)
 - Open to non ITU-T members
 - Proactive outreach to stakeholders from a wide range of areas – web services, NGN, user-centric identity and other SDOs were invited
 - Included highly active Identity Management developer community
 - Identity Commons
 - OpenID
 - Identity Gang
 - Windows CardSpace
 - Work conducted using mix of unstructured (OpenSpace) and structured legacy ITU-T standards meeting processes
 - A Wiki was established to allow for continuing autonomous group interaction and inputs and consensus building
 - <http://www.ituwiki.com>

- ITU-T Focus Group on Identity Management Report**
Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007
- Meeting input materials**
- Presentations
 - ITU-T SG13, SG17 & ISO SC27 (IdM) – R Brackney and A Rutkowski
 - NGN – A Rutkowski (VeriSign)
 - Content Industry Standards Identifier Activities – N Paskin (ISO)
 - Handle System – N Paskin (ISO)
 - 3GPP IdM Related Activities – M Euchner (Siemens-Nokia)
 - Liberty Alliance – Fulup Ar Foll (Sun)
 - Card Space and Identity Meta System – M Jones (Microsoft)
 - OpenID – D Recordon (VeriSign)
 - OASIS XRI (i-names) and XDI – A Madhok (Amsoft)
 - Higgins – A Nadalin (IBM)
 - JCA-NID (RFID/Sensor Identification) – P-A Probst (Swiss OFCOM)
 - OID (Object Identifier Registry) – O Dubuisson (France Telecom)
 - Identity Commons overview – K Hamlin (Identity Woman)

- ITU-T Focus Group on Identity Management Report**
Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007
- Meeting input materials**
- Meeting Contributions
 - IdM Discussion Items (Telcordia Technologies)
 - IdM example use case – eGovernment Services (Telcordia Technologies)
 - IdM example use case – Operational Response to Cyber Attacks (Telcordia Technologies)
 - IdM Mapping in other fora (VeriSign)
 - Liaisons
 - Other ITU-T Study Groups/forums
 - ETSI
 - ATIS
 - Demonstrations
 - I-Names/XRI (Amsoft)
 - Higgins Trust Framework (IBM)
 - VeriSign Identity Protection (VIP) - 3rd party managed CardSpace implementation using OpenID2 (VeriSign)
 - CardSpace Implementation (Microsoft)

- ITU-T Focus Group on Identity Management Report**
Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007
- Meeting Results**
- More than 50 participants from multiple IdM communities and countries
 - Successful adaptation to new methods and dialogue
 - Aggressive meeting schedule and consensus-based deliverables thru 2007 that meet latest Terms of Reference
 - global analysis of IdM requirements and capabilities
 - oriented around effective means for resource discovery and interoperation
 - includes living list of implementation requirements, especially privacy
 - generic IdM Framework including data models and related schemas,
 - includes identifying gaps in applicable specifications of standards bodies, forums, and consortia working on identity management
 - use case scenarios, including those related to critical infrastructure protection and operational response to cyber attacks
 - global IdM organization living list including compilation of a common IdM lexicon



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Assumptions and Value Propositions

- **Assumptions**
 - Multiplicity and contextual nature of identities
 - Security of network infrastructure, applications/services and user
 - Focus on reuse rather than reinvention
 - Will not produce new specifications for national credentials for persons
- **Value Propositions for Business and Users**
 - Making possible entirely new user experiences and business opportunities based on emergence of a global identity/social layer
 - Unlocking or leveraging latent value of social/identity infrastructure
 - Making the user's life easier, privacy-respecting, and more secure in the digital world
 - Ability to network securely, and exchange information across domains
 - Reduce cost through the reuse of existing infrastructure



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Initial Structure – Working Groups

- **Framework Architecture** – Chairs: Tony Nadalin (IBM) and Scott Cadzow (ETSI STF)
 - Data Model – Leaders: Tony Nadalin (IBM), Paul Trevithick (Parity Communications)
 - Requirements – Leaders: Piotr Pacyna (Universidad Carlos III)
 - Use Cases – Leaders: Sergio Fiszman (Nortel), Mike Jones (Microsoft), Lee Dryburgh (University College of London)
 - Architecture – Leaders: Sergio Fiszman (Nortel), Zacharias Zeltsan (Alcatel-Lucent)
- **Discovery and Assurance Metrics** – Chairs: Tony Rutkowski (VeriSign) and Lee Dryburgh (University College of London)
- **Organizations and Lexicon** – Chair: Mike Hind (CESG)
- **Legal Requirements, including Privacy** – Chair: Tony Rutkowski (Verisign)

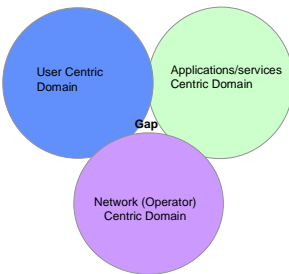


ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Consensus on Nature of the IdM Gap

- Current state of IdM is that it is being viewed and addressed in a disconnected manner (i.e., silos) from the following perspectives:
 - User-centric perspective (e.g., capabilities to allow user control of personal identifiers, roles and privacy attributes),
 - Applications/services (e.g., applications and services developers)
 - Network (e.g., service and infrastructure providers).
- Each domain is being independently developed for specific near-term / first-to-market needs, without consideration for the value/need for interoperability and harmonization.



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Consensus on Potential Interoperability

- Gaps are related to the exchange, correlation and linkage of the identity related information between the different planes (user, application/service and network)
- Includes
 - Data model for exchange (pull and push) of identity related information between the network and application/service (e.g., application requesting and the network providing location or network address information as generic objects)
 - Architectural model to allow correlation of the identity related functions in the different planes (e.g., user control process, application process and network functions) to allow interoperability (i.e., bridging of existing functions and capabilities) and adherence to policy controls
 - Model to support user control of certain network related preferences (e.g., user control of network/service provider preferences and privacy attributes)



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Cyberprotection operational use case

- As IdM capabilities and services begin to be supported by the public and enterprise network infrastructures, both end users and service providers will continue to be subjected to cyber attacks, as well as attacks specifically focused on IdM systems, capabilities and services as they are deployed.
- **Scenarios include**
 - Use of IdM capabilities to identify, protect and respond to cyber attacks generally
 - Response to attack on IdM infrastructure itself

From Telcordia IdM FG Doc. 11



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Value of IdM Information Sharing and Coordination

- Significant value for the attacked service provider to share information and coordinate across its enterprise and with other services providers (ISACs) and Computer Emergency Response Teams (CERTs) both nationally and internationally, in a trusted manner
 - to determine if an attack is focused or broad-based, and if other service providers have IdM elements that affect the attacked service provider necessitating action to partition off the attack
 - Attacked service provider should provide other service and network providers attack information to check if they are affected and prevent propagation of attack vector
 - Coordination may leverage existing cyber security coordination mechanisms, or may require new coordination procedures
- IdM capabilities can be leveraged to facilitate rapid coordination and sharing of information based on pre-established and authenticated trust relationships
 - a separate trusted database can be created that coordinates information regarding IdM related cyber attacks
 - Allows coordinated sharing and response
 - IdM can be used to authenticate responding service providers and ISACs / CERTs
 - use IdMs to authenticate Network Elements to validate relationships between network elements to ensure the legitimacy of the transactions

From Telcordia IdM FG Doc. 11



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Identified International IdM Public R&D/Standards Initiatives

- **European Union R&D Consortia**
 - **6th Framework Programme 2002-2006**
 - Daidalos (www.st-daidalos.org)
 - Focused on network IdM platforms
 - GUIDE (www.guide-project.eu)
 - Focused on a conceptual framework for eGovernment IdM
 - Modiris (www.csis.org/eu/en/activities/identitymodiris.htm)
 - Focused on eGovernment IdM in the EU pursuant to the 2010 plan
 - PRIME (www.prime-project.eu)
 - Focused on privacy-enhancing Identity Management Systems
 - **7th Framework Programme 2007-2008**
 - €9.1 billion for funding ICT
 - FP7-ICT-2007-1: Objective ICT-2007.1.4: Secure, dependable and trusted Infrastructures
 - Identity management and privacy enhancing tools
 - FP7-ICT-2007-1: Objective ICT-2007.1.6: New Paradigms and Experimental Facilities
 - trust and identity management architectures and technologies
- **European Union Standards**
 - **ETSI Specialist Task Force QZ on Security and IdM in NGN**
 - Permanent expert staff to facilitate and develop standards-based IdM solutions
- **Korea**
 - **ETRI** (http://www.etri.re.kr/www_05/e_etri/)
 - Focused primarily on IdM of RFID and objects under the aegis of Network Identity (NID)
 - Coordinating Japan, China, and Switzerland on NID



ITU-T Focus Group on Identity Management Report

Research & Development Task Force Meeting
CSC, Falls Church VA, 7 March 2007

Recommendations to NSTAC community

- IdM Focus Group provides unique opportunities to discover and analyze new IdM developments, participate, and shape global IdM infrastructure capabilities
 - Includes an enormous array of well-funded IdM R&D activities worldwide
 - Valuable to NSTAC and entire associated NS/EP community and industry
 - Opportunity to work directly with counterparts in other regions and countries
 - Builds directly on the Ottawa NSTAC 2006 RDX Workshop
- Impediments to participation are minimal
- R&D, analyses, and inputs are especially needed for CIP and NS/EP related IdM capability requirements




Disclaimer: The views herein expressed are those of the presenter and not necessarily those of VeriSign or any other institution with whom he may be affiliated.

ISS World
Intelligence Support Systems for Lawful Interception, Cyber Investigations and Intelligence Analysis for Europe, Middle East, Africa and Asia
25-28 FEBRUARY 2007 • DUBAI, UAE

V1.2

Keynote Address
Dubai, 26 Feb 2007

State of ISS February 2007: Principal Developments



Anthony M Rutkowski
Vice President for Regulatory Affairs and Standards
Dulles VA USA
tel: +1 703.948.4305
mailto:trutkowski@verisign.com
*President, Global LI Industry Forum
Distinguished Senior Research Fellow, Center for International Strategy Technology and Policy, Georgia Tech*

Where it all comes together.

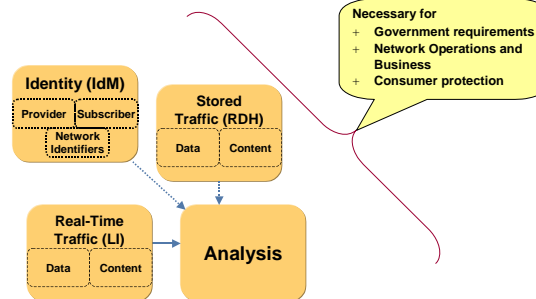
Principle Recent Developments

- + **Meta developments**
 - ? Cybercrime Convention update: 19 enter into force (Armenia, Iceland, Netherlands, and USA as of 1 Jan 2007); 43 signed; community of excellence grows
 - ? 164 countries sign ITU treaty *Final Acts* including multiple security resolutions
 - ? Continued integration of industry, government, and consumer needs for effective network forensic capabilities
- + **Lawful Interception (LI)**
 - ? National authorities proceed with new Internet/NGN requirements
 - ? Compliance-on-Demand solutions appear in the marketplace
 - ? Standards committees develop LI specifications and techniques, introduce controversies
 - Time-stamp accuracy, internationalization, standards & module availability, syntax languages, secure buffering, Direct Signal Reporting, evolution and extensibility
- + **Retained Data Handover (RDH)**
 - ? Multiple nations now developing and cooperating on retained data requirements
 - ? Industry-government RDH standards activity now formally organized within ETSI LI
- + **Identity Management (IdM)**
 - ? Widespread recognition of profound IdM needs for Internet/wireless/NGN infrastructure
 - ? National authorities together with industry adopt programs manifested through ITU-T, ISO, and many other forums
 - ? Identity Management mandates still lacking
 - ? Windows Vista bundles CardSpace

Cybercrime/Cybersecurity Response

- + **Kyiv Conference, 6-7 Feb 2007**
 - ? Council of Europe and the European Commission support Ukraine as followup to Cybercrime Convention ratification
 - ? CoE Sec-Gen statement regarding child predators in cyberspace and Convention being open to additional signatories
- + **ITU Plenipotentiary Conference (Antalya, 2006), SPU**
 - ? RES 71 *Strategic plan for the Union for 2008-2011*
 - ? RES 130 *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*
 - ? RES 149 *Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies*
 - ? SPU global updates www.itu.int/osg/spu/cybersecurity/pgc/
- + **Infrastructure Protection Initiatives**
 - ? EPCIP – European Programme for Critical Infrastructure Protection
 - Activity led by Directorate-General for Justice, Freedom and Security (JLS)
 - ? APEC TEL/SEC ISTWG + SCADA
 - ? USA NSTAC programme on CIP
- + **Analytical capabilities becoming commercial offerings**
 - ? VeriSign *iDefense* services

The network forensics Rosetta Stone



Meta: integration of NGN needs

- + **Availability, security, and legal**
 - ? Maintaining high availability, minimizing outages; services restoration
 - ? *Priority access capabilities*
 - ? Assistance to law enforcement (LI, data retention, cybercrime mitigation)
 - ? Public Safety (E911, emergency alerts)
 - ? Digital rights management
 - + **Competition**
 - ? Unbundling
 - ? Interoperability
 - ? Nominadity (number portability, roaming)
 - + **Operations**
 - ? Identity Management
 - ? Inter-carrier compensation
 - ? Billing and accounting
 - + **Consumer**
 - ? Universal service
 - ? Preventing intrusions (DoNotCall, CallerID)
 - ? CPNI protection and privacy
 - ? Disability assistance
 - ? Fraud management

Synergy
Capabilities for supporting ISS requirements are common to nearly all
- Increasingly, governments are integrating staff units to deal with these needs together, e.g.,
EC JLS Directorate
USA FCC Public Safety and Homeland Affairs Bureau

LI: the USA market - proceeding with new Internet/NGN requirements

- + **LI compliance required for 1) Internet broadband access, and 2) interconnected VoIP providers**
 - ? FCC estimates 5,920 providers affected; 14,141 Form 445 filings
 - ? Initial CALEA Monitoring Report for Broadband and VoIP Services (Form 445) was due on 12 Feb 2007
 - ? FCC Rules § 1.20005 policies and procedures filing is due 12 March 2007
- + **Simple options**
 - ? Will provider be compliant by 14 May 2007
 - ? If not, why not
 - ? Three options: self-implemented industry standard compliance; self-implemented custom solution approved by DOJ; Trusted Third Party
- + **Compliance moved to new FCC Public Safety and Homeland Security Bureau**
 - ? Bolstered with substantial investigative capabilities and imposition of penalties
 - ? Emphasized by numerous enforcement actions for other mandates
- + **FCC 3rd Report and Order** will treat obligations of significant private IP network providers and other remaining issues

LI: Compliance-on-Demand solutions

- + "Compliance-on-demand" (CoD) solutions are being discussed/proffered in the USA LI marketplace
- + Less than fully compliant under the FCC Rules
 - ? Rely on some manner of
 - Installation readiness
 - Cache of readily available equipment
- + Benefits
 - ? A potentially attractive alternative for some providers and architectures
 - Highly distributed access points
 - Locations with low expectations of intercept orders, especially private networks
- + Difficulties
 - ? Loss of immediate exigent capabilities for law enforcement that are becoming increasingly common in highly nomadic Internet environments
 - ? Technical and operational complexities of assuring Compliance-on-Demand solutions will work; what proof-of-performance is necessary
 - ? Administrative and enforcement complexities



LI: standards committee work

- + ETSI LI Technical Committee
 - ? de facto global body for most LI standards and collaboration
 - ? LI standards center of excellence; best of breed solutions
 - Large, diverse industry participation
 - Standards and syntax code openly available, extensively tested, and in proper "trees"
 - Interoperability tests using new standards completed
 - Regularly evolved
 - ? Recently completed WiFi intercept standard; assumed NGN, cable, and retained data standards projects; started IP-TV
- + 3GPP SA Technical Committee
 - ? GSM/IMS/Next Gen wireless LI standards; mobile packet data, WLAN, Multimedia Broadcast/MultiCast Service specs evolved
- + CableLabs
 - ? New Packet Cable 2.0 specification released; de facto global standards for cable
- + ATIS
 - ? PTSC/LAES working on USA LI standards for VoIP/Internet Access
 - ? WTSC/LI working on USA 3GPP adaptations



LI: time-stamp accuracy

- + Accurate time-stamps for network forensic events and national security are critical
 - ? For sequencing disparate events in an investigation
 - ? For analyzing criminal and terrorist behavior
 - ? For evidence in a criminal proceeding
- + Refusal of some standards bodies to adopt needed time-stamp requirements led the USA regulatory authority to enact 200 millisecond accuracy requirement in law
 - ? FCC 47 CFR §1.20007(a)(14) specifies that an Intercept Access Point call event be contemporaneously "time-stamped to an accuracy of at least 200 milliseconds"
- + Well understood professional and legal practice dictates accuracy measurements against national standards – coordinated globally by *Le Bureau international des poids et mesures (BIPM)* www.bipm.org
- + Accuracies of 10 milliseconds or better are commonplace in IP network operations and frequently used for incident analysis
 - ? Network Time Protocol (NTP) provides requisite accuracies, and is ubiquitous in the IP network infrastructure and essentially without cost
- + Government authorities need to assure needs for time-stamp accuracy are met



LI: emerging significant standards challenges

- + Internationalization
 - ? Maintaining separate standards in separate standards organizations for the USA drives up costs; drives down functionality and quality for vendors, USA providers and law enforcement
 - ? Necessary for increasing transnational LI support
- + Standards & module availability
 - ? Good standards practice, if not current law, dictates the public availability of standards documents, standards, and the code modules
- + Syntax languages
 - ? Most of the world has shifted to XML for information exchange while the LI handover interfaces remain the last vestige of ASN.1 syntax
- + Secure buffering
 - ? A new standards project to develop a trusted solution for delayed high bandwidth handovers could also support virtual points-of-presence
- + Direct Signal Reporting
 - ? Direct Signal Reporting (DSR) handover of signalling to law enforcement is emerging as preferable alternative
 - ? It is not possible in an IP NGN world to require providers to analyze and structure all call data
 - ? ETSI's TS102232 modular approach seems best for well-known services
- + Evolution and extensibility
 - ? Effective means are needed to deal with evolution of needs and standards and provide modular extensibility of capabilities specified
 - ? Mechanisms exist, especially in XML environment, but are not implemented



RDH: European Commission & National Mandates

- + EU Data Retention Directive still primary driver
 - ? EC to host major workshop 14 March 2007 at Brussels
 - ? Compliance required by 15 Sep 2007
 - ? Modulated by EU Member States; several such as Italy and France have proceeded on their own, Germany, Netherlands, Denmark, UK and others are implementing variants
- + Australia, Korea, Russia, and others have enacted similar data retention legislation
- + Some new legislative actions in USA – Smith Bill, H.R.837
- + Biggest beneficiaries may be both providers and law enforcement worldwide who will finally get a common global stored data handover interface to facilitate subpoena execution
- + Consumers could benefit from greater CPNI and privacy protection



RDH: ETSI LI to deliver Retained Data standards

- + Retained Data Handover standards work obtained major boost in June 2006
 - ? Retained Data standards effort moving forward
 - ? Chaired by Mark Shepherd (Detica, UK)
 - ? ETSI TC LI re-chartered to accommodate work
 - ? Meetings at Tenerife (30 Jan–1 Feb 2007); Rotterdam, (22-23 Mar 2007)
 - ? OASIS XML query-response model being pursued; significant implementations exist in judicial systems
- + Significant RDH Interface Issues
 - ? What are the common global LEA RDH requirements? (See ETSI DTS/LI-00039, doc. 1411td019)
 - ? Use of virtual versus real storage brings significant benefits for providers
 - ? How much processing to require on the provider side of the interface
 - ? How to implement future conditional court orders
 - ? How to manage and "publish" the diverse profiles for the RDH Interface
 - ? How to provision an "EU Art. 9 Supervisory Authority" interface

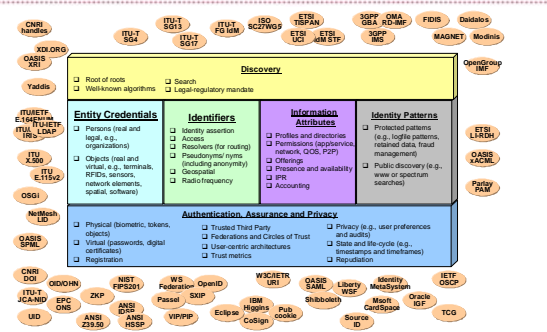


Identity Management: where the action is today

- + Far reaching developments unfolding in Identity Management (IdM) arena
- + Driven by a mix of government, industry operational, and consumer needs
 - ? Public IP enabled Next Generation Networks supporting nomadic, always-on everything, is not viable without baked-in global IdM capabilities
 - ? Key event represented by Bill Gates' February RSA keynote on CardSpace using OpenID and bundled with new Vista PC operating system
- + Occurring under the aegis of broad arrays of Next Generation Network (NGN) industry, technical and regulatory forums
 - ? National authorities with industry are adopting implementation requirements and frameworks manifested through ITU-T, ISO, NSTAC, and many other forums
- + Core product is the *Common Global Identity Management Framework* in ITU-T, ISO/IEC, and regional/national bodies
 - ? Major steps taken 2 weeks ago in Geneva with first meeting of IdM Focus Group
 - ? OpenSpace and Wiki based collaboration at www.ituwiki.com
 - ? Beijing Jan 2006 meeting produced initial draft Recommendation Y.IdMsec specification of framework
- + ISS community also needs these capabilities to remain functional



Identity Management Global Framework Ecosystem



Objective: A Common Global Identity Management Framework

- + Common global ability to
 - ? Rapidly discover and query authoritative source information for any entity's
 - identities, credentials, identifiers, communication routing, attributes, and patterns for any entity involved in a communication
 - ? Use a assurance trust metric and protocol associated with all identities and identifiers
- + "Entity" includes "anything that has separate and distinct existence that can be uniquely identified"
 - ? real persons, legal persons, objects, geospatial constructs, RFIDs, sensors, devices, software,...
- + Requires
 - ? Convergence on discovery and interoperability
 - ? Accommodation of diversity and autonomy
 - ? Extensibility to enable constant evolution
- + IdM critical for data retention implementation and network forensics "use cases" are emerging in IdM Focus Group



Distribution list

Document No.: DRDC CSS CR 2008-06

LIST PART 1: Internal Distribution by Centre:

- 1 David McKellar, Scientific Authority
- 1 CSS Library
- 1 Andrew Vallerand
- 1 Alain Goudreau
- 4 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

Dr. Robert Walker
ADM S&T
Réne Larose
DRDC CORP
COS
DRDCKIM
Lynelle Spring
Springworks Consulting
54 Qualicum St.
Ottawa, ON
K2H 7H4
Shane Roberts
S&T Policy Division
Public Safety Canada
269 Laurier Ave W
Ottawa, ON
K1A 0P8
Robert Crawhall
National Capital Institute of Telecommunications
200-2625 Queensview Dr.
Ottawa, ON
K2B 8K2

Jack Smith
Office of the National Science Advisor
235 Queen St.

Ottawa, ON
K1A 0H5

Ken Andrews
High Impact Facilitation 6 Elderwood Trail
Stittsville, ON
K2S 1C9

8 TOTAL LIST PART 2

12 TOTAL COPIES REQUIRED

DOCUMENT CONTROL DATA		
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		
1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED	
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.) Global Security Scan for Canadian Science Capabilities (2015-2020)		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Spring, Lynelle; Crawhall, Robert; Smith, Jack; Andrews, Ken		
5. DATE OF PUBLICATION March 2008	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 85	6b. NO. OF REFS (Total cited in document.) 3
7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Contractor Report		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)	

	W7714-6-09998
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC CSS CR 2008-06	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) Unlimited	
12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))	
13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)	
14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.) Risk Analysis, Global Security, Capability Based Planning, Cyber Security, Transportation Security, Critical Infrastructure Protection	